

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:)
Isao YAGASAKI, et al.)
Serial No.: To be assigned) Group Art Unit: Unassigned
Filed: December 28, 2000) Examiner: Unassigned



For: **MEMBERSHIP QUALIFICATION PROCESSING SYSTEM AND METHOD
THEREOF**

**SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN
APPLICATION IN ACCORDANCE
WITH THE REQUIREMENTS OF 37 C.F.R. §1.55**

*Assistant Commissioner for Patents
Washington, D.C. 20231*

Sir:

In accordance with the provisions of 37 C.F.R. §1.55, the applicants submit herewith a certified copy of the following foreign application:

Japanese Patent Application No. 2000-121582
Filed: September 29, 2000.

It is respectfully requested that the applicants be given the benefit of the foreign filing date as evidenced by the certified papers attached hereto, in accordance with the requirements of 35 U.S.C. §119.

Respectfully submitted,

STAAS & HALSEY LLP

By: 

James D. Halsey, Jr.

Registration No. 22,729

Date: December 28, 2000
700 11th Street, N.W., Ste. 500
Washington, D.C. 20001
(202) 434-1500



PATENT OFFICE
JAPANESE GOVERNMENT

This is to certify that the annexed is a true copy of the following application as filed with this office.

Date of Application: April 21, 2000

Application Number: Patent Application
No. 2000-121582

Applicant(s): FUJITSU LIMITED

September 29, 2000

Commissioner,
Patent Office Kozo Oikawa

Certificate No. 2000-3079683

日 本 国 特 許 庁

PATENT OFFICE
JAPANESE GOVERNMENT

JC654 U.S. PTO
09/749720
12/28/00

別紙添付の書類に記載されている事項は下記の出願書類に記載されて
いる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed
with this Office.

出 願 年 月 日

Date of Application:

2000年 4月21日

出 願 番 号

Application Number:

特願2000-121582

願 人

Applicant(s):

富士通株式会社

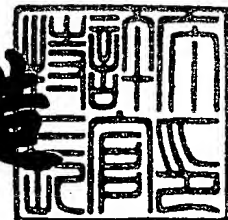
CERTIFIED COPY OF
SECURITY DOCUMENT

CERTIFIED COPY OF
SECURITY DOCUMENT

2000年 9月29日

特 許 庁 長 官
Commissioner,
Patent Office

及 川 耕 造



出証番号 出証特2000-3079683

【書類名】 特許願

【整理番号】 0050484

【提出日】 平成12年 4月21日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 15/00
H04L 9/32

【発明の名称】 入会審査のための処理システムおよび方法

【請求項の数】 13

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

【氏名】 矢ヶ崎 功

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

【氏名】 黒田 俊光

【特許出願人】

【識別番号】 000005223

【氏名又は名称】 富士通株式会社

【代理人】

【識別番号】 100074099

【住所又は居所】 東京都千代田区二番町8番地20 二番町ビル3F

【弁理士】

【氏名又は名称】 大菅 義之

【電話番号】 03-3238-0031

【選任した代理人】

【識別番号】 100067987

【住所又は居所】 神奈川県横浜市鶴見区北寺尾7-25-28-503

【弁理士】

【氏名又は名称】 久木元 彰

【電話番号】 045-573-3683

【手数料の表示】

【予納台帳番号】 012542

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9705047

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 入会審査のための処理システムおよび方法

【特許請求の範囲】

【請求項 1】 複数のサービスの加入条件を格納する格納手段と、

前記複数のサービスの加入条件のうち、ユーザが加入済みのサービスの加入条件と未加入のサービスの加入条件とを比較して、該ユーザが加入可能なサービスを選別する選別手段と、

前記加入可能なサービスの情報を前記ユーザに提示する提示手段とを備えることを特徴とする処理システム。

【請求項 2】 前記選別手段は、前記ユーザが複数のサービスに加入済みであるとき、複数の加入済みのサービスの加入条件を合算し、合算された加入条件と前記未加入のサービスの加入条件とを比較することを特徴とする請求項 1 記載の処理システム。

【請求項 3】 前記複数の加入済みのサービスに共通の証明書情報を登録する登録手段と、前記ユーザの証明書情報を受け取る受信手段とをさらに備え、前記選別手段は、該ユーザの証明書情報が該共通の証明書情報に対応するとき、該ユーザの証明書情報に基づいて、前記複数の加入済みのサービスの加入条件を取得することを特徴とする請求項 2 記載の処理システム。

【請求項 4】 あるサービスの入会審査のための判断基準情報として、他のサービスの識別情報を格納する格納手段と、

ユーザが前記あるサービスへの入会を希望するとき、該ユーザが前記他のサービスを利用しているか否かを判定する判定手段と、

前記ユーザが前記他のサービスを利用しているとき、該ユーザが前記あるサービスへの入会資格を有すると判断する判断手段とを備えることを特徴とする処理システム。

【請求項 5】 前記ユーザが利用しているサービスのための証明書情報を登録する登録手段と、前記ユーザの証明書情報の識別情報を受け取る受信手段とをさらに備え、前記判定手段は、該識別情報が登録された証明書情報に対応するとき、該識別情報に基づいて、該ユーザが利用しているサービスの情報を取得し、

該ユーザが前記他のサービスを利用しているか否かを判定することを特徴とする請求項 4 記載の処理システム。

【請求項 6】 既存のサービスの加入条件を格納する格納手段と、
新たな加入条件を設定する設定手段と、
前記既存のサービスの加入条件と新たな加入条件とを比較して、該新たな加入条件で加入可能なユーザの数に関する情報を求めるシミュレーション手段と、
得られた情報を出力する出力手段と
を備えることを特徴とする処理システム。

【請求項 7】 前記既存のサービスを利用している複数のユーザの証明書情報を登録する登録手段をさらに備え、前記シミュレーション手段は、前記新たな加入条件が前記既存のサービスの加入条件を満たすとき、該証明書情報の数をカウントして、前記加入可能なユーザの数を求めることを特徴とする請求項 6 記載の処理システム。

【請求項 8】 コンピュータのためのプログラムを記録した記録媒体であって、

前記プログラムは、
複数のサービスの加入条件のうち、ユーザが加入済みのサービスの加入条件と未加入のサービスの加入条件とを比較して、該ユーザが加入可能なサービスを選別し、

前記加入可能なサービスの情報を前記ユーザに提示する
処理を前記コンピュータに実行させることを特徴とするコンピュータ読み取り可能な記録媒体。

【請求項 9】 コンピュータのためのプログラムを記録した記録媒体であって、

前記プログラムは、
ユーザがあるサービスへの入会を希望するとき、該あるサービスの入会審査のための判断基準情報に含まれる他のサービスの識別情報に基づいて、該ユーザが該他のサービスを利用しているか否かを判定し、

前記ユーザが前記他のサービスを利用しているとき、該ユーザが前記あるサー

ビスへの入会資格を有すると判断する

処理を前記コンピュータに実行させることを特徴とするコンピュータ読み取り可能な記録媒体。

【請求項 1 0】 コンピュータのためのプログラムを記録した記録媒体であって、

前記プログラムは、

新たな加入条件を設定し、

既存のサービスの加入条件と前記新たな加入条件とを比較して、該新たな加入条件で加入可能なユーザの数に関する情報を求め、

得られた情報を出力する

処理を前記コンピュータに実行させることを特徴とするコンピュータ読み取り可能な記録媒体。

【請求項 1 1】 複数のサービスの加入条件を蓄積し、

前記複数のサービスの加入条件のうち、ユーザが加入済みのサービスの加入条件と未加入のサービスの加入条件とを比較して、該ユーザが加入可能なサービスを選別し、

前記加入可能なサービスの情報を前記ユーザに提示することを特徴とする処理方法。

【請求項 1 2】 ユーザがあるサービスへの入会を希望するとき、該あるサービスの入会審査のための判断基準情報を参照し、

前記判断基準情報に含まれる他のサービスの識別情報に基づいて、前記ユーザが該他のサービスを利用しているか否かを判定し、

前記ユーザが前記他のサービスを利用しているとき、該ユーザが前記あるサービスへの入会資格を有すると判断する

ことを特徴とする処理方法。

【請求項 1 3】 サービスの加入条件とユーザ数の関係のシミュレーションを行う処理方法であって、

新たな加入条件を設定し、

既存のサービスの加入条件と前記新たな加入条件とを比較して、該新たな加入

条件で加入可能なユーザの数に関する情報を求める
ことを特徴とする処理方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、インターネット等のネットワークを介した会員制サービスに係り、ユーザが複数のサービスを利用する際、各サービスの入会審査に関する処理を行うシステムおよび方法に関する。

【0002】

【従来の技術】

ネットワーク上のサービスを提供する提供者は、サービス料金の課金等のために、アクセスしてきたユーザの認証を行う必要がある。従来のサービスシステムでは、1人のユーザが複数のサービスを利用する場合、各サービスが指定する認証方法をユーザ自らが使い分けていた。

【0003】

図29は、このような従来のサービスシステムを示している。2つのサービスA、Bを利用するとき、ユーザ11は、まず、サービスA用の識別情報(ID)とパスワード(PWD)をサービスAのサーバ12に送る。サーバ12は、ユーザ管理データベース(ユーザ管理DB)13を参照してユーザ認証を行った後、ユーザ11にサービスAを提供する。

【0004】

次に、ユーザ11は、サービスB用のIDおよびパスワードをサービスBのサーバ14に送る。サーバ14は、ユーザ管理DB15を参照してユーザ認証を行った後、ユーザ11にサービスBを提供する。こうして、ユーザ11は、ネットワークサービスA、Bを利用することができる。

【0005】

【発明が解決しようとする課題】

しかしながら、上述した従来のサービスシステムには、次のような問題がある。

【 0 0 0 6 】

1人のユーザが複数の会員制サービスを利用する場合、サービス毎に入会審査を受ける必要があり、そのために指定された個人情報を端末から入力しなければならない。したがって、利用サービスの数が多くなると、ユーザの負担が増大する。

【 0 0 0 7 】

また、各サービスを提供する事業体は、ユーザ毎に入会審査を行う必要があり、そのためにユーザから送られた個人情報を分析しなければならない。したがって、入会希望ユーザの数が多くなると、入会審査の負荷が増大する。

【 0 0 0 8 】

さらに、各事業体は、新たなサービスを開始するとき、どの程度の会員が集められるかを予測しながら、入会審査に用いる条件を設定する必要がある。このとき、設定条件と会員数の関係を効率良く分析するシステムが望まれる。

【 0 0 0 9 】

本発明の課題は、ユーザが複数の会員制サービスを利用する場合に、各サービスの入会審査に関する処理を効率化するシステムおよび方法を提供することである。

【 0 0 1 0 】

【課題を解決するための手段】

図1は、本発明の処理システムの原理図である。

本発明の第1の局面において、処理システムは、格納手段21、選別手段22、および提示手段23を備える。格納手段21は、複数のサービスの加入条件を格納する。選別手段22は、複数のサービスの加入条件のうち、ユーザが加入済みのサービスの加入条件と未加入のサービスの加入条件とを比較して、ユーザが加入可能なサービスを選別する。提示手段23は、得られた加入可能なサービスの情報をユーザに提示する。

【 0 0 1 1 】

ユーザが加入可能なサービスの情報を希望したとき、選別手段22は、格納手段21に格納された加入条件から、そのユーザが加入済みのサービスの加入条件

と未加入のサービスの加入条件を抽出する。そして、それらを比較することにより、未加入のサービスから加入可能なサービスを選別して、選別結果を提示手段 2 3 に渡す。提示手段 2 3 は、受け取った選別結果に含まれる加入可能なサービスの一覧を、ユーザに提示する。

【 0 0 1 2 】

このような処理システムによれば、ユーザは、入会審査を受ける前に、加入可能なサービスの一覧を取得することができる。したがって、すべての未加入サービスの入会審査を受けなくても、加入可能サービスを絞り込むことができ、その中から加入サービスを効率良く選択することができる。

【 0 0 1 3 】

また、本発明の第 2 の局面において、処理システムは、格納手段 2 1、判定手段 2 4、および判断手段 2 5 を備える。格納手段 2 1 は、あるサービスの入会審査のための判断基準情報として、他のサービスの識別情報を格納する。判定手段 2 4 は、ユーザがあるサービスへの入会を希望するとき、ユーザが他のサービスを利用しているか否かを判定する。判断手段 2 5 は、ユーザが他のサービスを利用しているとき、そのユーザがあるサービスへの入会資格を有すると判断する。

【 0 0 1 4 】

ユーザがあるサービスへの入会を希望するとき、判定手段 2 4 は、格納手段 2 1 に格納された、そのサービスの入会審査のための判断基準情報を参照して、その判断基準情報に含まれる他のサービスの識別情報を取得する。そして、その識別情報に基づいて、ユーザが他のサービスを利用しているか否かを判定し、判定結果を判断手段 2 5 に渡す。その判定結果が、ユーザが他のサービスを利用していることを表すとき、判断手段 2 5 は、そのユーザが入会資格を有すると判断する。

【 0 0 1 5 】

このような処理システムによれば、ユーザが新たなサービスに入会するとき、ユーザの個人情報の代わりに、同じような加入条件を設定している他のサービスへの入会状況に基づいて、入会資格の有無を判断することができる。したがって、入会審査が簡便化され、サービス運用者の負荷が軽減される。

【 0 0 1 6 】

また、本発明の第 3 の局面において、処理システムは、格納手段 2 1、設定手段 2 6、シミュレーション手段 2 7、および出力手段 2 8 を備える。格納手段 2 1 は、既存のサービスの加入条件を格納する。設定手段 2 6 は、新たな加入条件を設定する。シミュレーション手段 2 7 は、既存のサービスの加入条件と新たな加入条件とを比較して、新たな加入条件で加入可能なユーザの数に関する情報を求める。出力手段 2 8 は、得られた情報を出力する。

【 0 0 1 7 】

サービス運用者は、サービスの加入条件とユーザ数の関係を分析したいとき、設定手段 2 6 を用いて、新たな加入条件を設定する。シミュレーション手段 2 7 は、格納手段 2 1 に格納された既存のサービスの加入条件と、設定された加入条件とを比較して、設定された加入条件を有するサービスに加入可能なユーザの数等を求める。そして、出力手段 2 8 は、設定された加入条件と得られたユーザの数の関係を出力する。

【 0 0 1 8 】

このような処理システムによれば、サービス運用者は、新たなサービスを開始するとき、あるいは、既存のサービスの加入条件を変更するときに、加入可能なユーザの数を考慮しながら、入会審査に用いる加入条件を効率良く設定することができる。したがって、サービス運用者の負荷が軽減される。

【 0 0 1 9 】

例えば、図 1 の格納手段 2 1 は、後述する図 1 0 のサービス管理 DB 5 2 に対応し、選別手段 2 2、提示手段 2 3、判定手段 2 4、判断手段 2 5、設定手段 2 6、シミュレーション手段 2 7、および出力手段 2 8 は、図 1 0 の証明書管理部 5 1 に対応する。

【 0 0 2 0 】

【発明の実施の形態】

以下、図面を参照しながら、本発明の実施の形態を詳細に説明する。

本実施形態のサービスシステムは、デジタル証明書に基づく認証システムを含み、独立した複数のネットワークサービスに対して、ユーザが 1 つのデジタル証

明書を提示することで、それらのサービスの利用が許可される。このデジタル証明書は、所定の認証方法により認証されたユーザのみに対して発行され、そのユーザが複数のサービスを利用可能であることを表す。

【 0 0 2 1 】

デジタル証明書は、ITU-T (International Telecommunication Union Telecommunication Standardization Sector) の仕様 X. 509 に基づき、ユーザ名、証明書発行者名、シリアル番号、ユーザの公開鍵等の情報を統合したデータに、認証局 (Certificate Authority) のデジタル署名を施すことで生成される。この証明書は、中に収められている公開鍵がそこに記されたユーザのものであることを証明している。

【 0 0 2 2 】

図 2 は、このような認証システムにおけるデジタル証明書の発行と審査を示している。図 2 において、サービス A、B は、ID およびパスワードを用いる会員制サービスに対応し、それぞれ、サーバ 3 2、3 3 からユーザ 3 1 に対して提供される。認証局 3 4 は、これらのサービスの事業体とは独立した証明書発行機関であり、ユーザ 3 1 に対して、サービス A、B に共通のデジタル証明書（共通証明書）を発行する。

【 0 0 2 3 】

共通証明書を用いた認証を可能にするためには、あらかじめ、認証局 3 4 がユーザ 3 1 に対してその共通証明書を発行する必要がある。ここでは、認証局 3 4 は、サービス A を介して共通証明書を発行し、サービス B に対する最初のアクセス時に、サーバ 3 3 がその共通証明書を審査する。サーバ 3 2、3 3 は、それぞれ、ユーザ情報管理テーブル 3 6、3 7 を保持しており、これらのテーブルには、あらかじめ、ユーザ 3 1 の ID、パスワード等が登録されている。この場合、以下のシーケンスに従って処理が行われる。

【 0 0 2 4 】

P 1 : ユーザ 3 1 は、サービス A 用の ID およびパスワードをサーバ 3 2 に送る。サーバ 3 2 は、ユーザ情報管理テーブル 3 6 を参照してユーザ認証を行い、認証結果が OK であれば、認証局 3 4 に共通証明書の発行を依頼する。

【 0 0 2 5 】

P 2 : サーバ 3 2 は、認証局 3 4 から共通証明書を受け取り、それをユーザ 3 1 に対して発行する。この段階では、ユーザ 3 1 が保持する共通証明書は、サービス A を利用する資格のみを有し、認証局 3 4 の証明書管理 DB 3 5 には、共通証明書の識別情報（例えば、シリアル番号）とともに、対応するユーザ名と、サービス A が利用可能であることを示す情報が登録される。また、ユーザ情報管理テーブル 3 6 には、ID およびパスワードとともに、その共通証明書のシリアル番号（Ser. No.）が登録される。

【 0 0 2 6 】

P 3 : ユーザ 3 1 は、発行された共通証明書をサーバ 3 3 に提示する。

P 4 : サーバ 3 3 は、提示された共通証明書ではサービス B が利用できないと判断し、ユーザ 3 1 にサービス B 用の ID およびパスワードを要求する。

【 0 0 2 7 】

P 5 : ユーザ 3 1 は、サービス B 用の ID およびパスワードをサーバ 3 3 に送る。

P 6 : サーバ 3 3 は、ユーザ情報管理テーブル 3 7 を参照してユーザ認証を行い、認証結果が OK であれば、サービス B をユーザ 3 1 に提供する。これ以降、ユーザが保持する共通証明書でも、サービス B の利用が可能となる。この段階では、ユーザが保持する共通証明書は、サービス A とサービス B を利用する資格を有し、証明書管理 DB 3 5 には、サービス A、B が利用可能であることを示す情報が登録される。また、ユーザ情報管理テーブル 3 7 には、ID およびパスワードとともに、共通証明書のシリアル番号が登録される。

【 0 0 2 8 】

ここでは、P 1 および P 5 の処理において、ID およびパスワードによるユーザ認証を行っているが、指紋情報、声紋情報、画像情報等による他の認証方法を用いてもよい。また、ユーザは、サービスの利用中止を希望する場合、共通証明書の失効またはサービスの利用禁止の手続きを行う。共通証明書の失効手続きを行う場合、図 3 に示すように、以下のシーケンスに従って処理が行われる。

【 0 0 2 9 】

P 1 1 : ユーザ 3 1 は、サービス A 用の I D およびパスワード、あるいは共通証明書を、サーバ 3 2 に送る。

P 1 2 : I D およびパスワードを受け取った場合、サーバ 3 2 は、ユーザ情報管理テーブル 3 6 を参照してユーザ認証を行い、認証結果が O K であれば、その旨をユーザ 3 1 に通知する。また、共通証明書を受け取った場合、サーバ 3 2 は、後述する認証方法でユーザ認証を行い、認証結果をユーザ 3 1 に通知する。

【 0 0 3 0 】

P 1 3 : ユーザ 3 1 は、サーバ 3 2 に対して、保持している共通証明書の失効依頼を行う。サーバ 3 2 は、認証局 3 4 に共通証明書のシリアル番号を通知し、失効処理を依頼する。認証局 3 4 は、証明書管理 D B 3 5 からその共通証明書の情報を削除し、サーバ 3 2 は、ユーザ情報管理テーブル 3 6 からその共通証明書のシリアル番号を削除する。

【 0 0 3 1 】

P 1 4 : その後、ユーザ 3 1 は、保持している共通証明書を、認証情報としてサーバ 3 3 に提示する。サーバ 3 3 は、提示された共通証明書のシリアル番号を認証局 3 4 に通知し、その共通証明書の正当性を問い合わせる。

【 0 0 3 2 】

P 1 5 : 認証局 3 4 は、通知されたシリアル番号が証明書管理 D B 3 5 に登録されていないため、チェック結果が N G であることをサーバ 3 3 に通知する。サーバ 3 3 は、ユーザ情報管理テーブル 3 7 からその共通証明書のシリアル番号を削除し、サービス B が利用不可であることをユーザ 3 1 に通知する。

【 0 0 3 3 】

図 4 は、発行された共通証明書を用いたユーザ認証を示している。この場合、以下のシーケンスに従ってサービスが提供される。

P 2 1 : ユーザ 3 1 は、保持している共通証明書を、認証情報としてサーバ 3 2 に提示する。サーバ 3 2 は、提示された共通証明書のシリアル番号を認証局 3 4 に通知し、その共通証明書のチェックを依頼する。認証局 3 4 は、証明書管理 D B 3 5 を参照して、通知されたシリアル番号が登録されているか否かをチェックする。そして、そのシリアル番号が登録されており、かつ、サービス A が利用

可能であれば、チェック結果としてOKを返す。

【0034】

P22：サーバ32は、認証局34からOKが返されると、サービスAをユーザ31に提供する。

P23：ユーザ31は、保持している共通証明書を、認証情報としてサーバ33に提示する。サーバ33は、サーバ32と同様にして、認証局34からチェック結果を受け取る。

【0035】

P24：サーバ33は、認証局34からOKが返されると、サービスBをユーザ31に提供する。

ここでは、ユーザが2つのサービスを利用する場合について説明したが、3つ以上のサービスを利用する場合も同様である。また、サーバ32、33は、提示された共通証明書が失効しているか否かを確認するために、認証局34に対して共通証明書のチェックを依頼しているが、このチェックを省略することも可能である。

【0036】

この場合、失効処理において、認証局34は、失効した共通証明書のシリアル番号を、関連するすべてのサービスのサーバに通知し、各サーバは、ユーザ情報管理テーブルからそのシリアル番号を削除する。そして、ユーザから共通証明書が提示されたとき、そのシリアル番号が対応するユーザ情報管理テーブルに登録されていれば、認証結果をOKとし、それが登録されていなければ、認証結果をNGとする。

【0037】

図2、3、および4に示した認証システムによれば、ユーザは、各サービス固有のIDおよびパスワードを使用することなく、単一の証明書を提示するだけで、複数のサービスを利用することができる。したがって、複数のIDおよびパスワードを暗記したり、サービス利用時に毎回IDおよびパスワードを入力したりする必要がなくなり、ユーザの負担が大きく軽減される。

【0038】

ところで、証明書管理DB35には、例えば、図5のような証明書管理テーブルと、図6のような利用サービス管理テーブルが格納される。図5の証明書管理テーブルには、共通証明書のシリアル番号、ユーザの氏名、住所、およびメールアドレスが登録されており、図6の利用サービス管理テーブルには、共通証明書のシリアル番号および利用可能サービスIDが登録されている。証明書管理テーブルおよび利用サービス管理テーブルは、共通証明書毎に生成される。

【0039】

また、図7は、ユーザ情報管理テーブル36、37の例を示している。図7のユーザ情報管理テーブルには、ユーザID、パスワード、ユーザの氏名、住所、および共通証明書のシリアル番号が登録されている。ユーザ情報管理テーブルは、ユーザ毎に生成される。

【0040】

図8は、ユーザ31がサービスAのサーバ32に対して、共通証明書の発行または失効を依頼する場合の処理のフローチャートである。まず、ユーザ31は、サーバ32にアクセスし（ステップS1）、サーバ32は、ユーザ端末にログイン画面を表示する（ステップS2）。次に、ユーザ31は、サービスA用のIDおよびパスワードを入力し（ステップS3）、サーバ32は、ユーザ情報管理テーブル36を参照して、入力されたIDおよびパスワードをチェックする（ステップS4）。

【0041】

IDおよびパスワードが正しくなければ、サーバ32は、ステップS2以降の処理を繰り返す。IDおよびパスワードが正しければ、次に、ユーザ情報管理テーブル36を参照して、対応するユーザに対して共通証明書が発行されているか否かをチェックする（ステップS5）。

【0042】

ユーザ情報管理テーブル36に、そのユーザの共通証明書のシリアル番号が登録されていなければ、共通証明書が発行されていないと判断し、認証局34に共通証明書の発行を依頼する（ステップS6）。

【0043】

これを受けて、認証局 3 4 は、共通証明書を発行する（ステップ S 7）。このとき、認証局 3 4 は、共通証明書のシリアル番号とユーザ情報を記録した証明書管理テーブルを生成し、共通証明書のシリアル番号とサービス A の ID を記録した利用サービス管理テーブルを生成する。そして、それらのテーブルを証明書管理 DB 3 5 に格納する。

【 0 0 4 4 】

次に、サーバ 3 2 は、発行された共通証明書をユーザ 3 1 に配布し、ユーザ情報管理テーブル 3 6 に、共通証明書のシリアル番号を記録して（ステップ S 8）、処理を終了する。

【 0 0 4 5 】

ステップ S 5 において、ユーザ情報管理テーブル 3 6 に共通証明書のシリアル番号が登録されていれば、共通証明書が発行済みであることをユーザ 3 1 に通知し、失効を希望するか否かを問い合わせる（ステップ S 9）。ユーザ 3 1 が失効を希望しなければ、そのまま処理を終了する。

【 0 0 4 6 】

ユーザ 3 1 が失効を希望すれば、登録されている共通証明書のシリアル番号を認証局 3 4 に通知し、失効処理を依頼する（ステップ S 1 0）。これを受けて、認証局 3 4 は、通知されたシリアル番号に対応する証明書管理テーブルおよび利用サービス管理テーブルを削除し、処理結果をサーバ 3 2 に通知する。そして、サーバ 3 2 は、ユーザ情報管理テーブル 3 6 からその共通証明書のシリアル番号を削除し、共通証明書が失効したことをユーザ 3 1 に通知して、処理を終了する。

【 0 0 4 7 】

次に、図 9 は、ユーザ 3 1 がサービス B のサーバ 3 3 に対して、保持している共通証明書の審査を依頼する場合の処理のフローチャートである。まず、ユーザ 3 1 は、サーバ 3 3 にアクセスし（ステップ S 1 1）、共通証明書を提示する（ステップ S 1 2）。

【 0 0 4 8 】

次に、サーバ 3 3 は、提示された共通証明書のシリアル番号がユーザ情報管理

テーブル 37 に登録されているか否かをチェックする（ステップ S 13）。そして、そのシリアル番号が登録されていなければ、ステップ S 14～S 16 において、図 8 のステップ S 2～S 4 と同様の処理を行う。

【0049】

ステップ S 16 において、ID およびパスワードが正しければ、次に、サーバ 33 は、提示された共通証明書のシリアル番号を認証局 34 に通知し、その共通証明書によるサービス B の利用許可を要請する（ステップ S 17）。

【0050】

これを受けて、認証局 34 は、通知されたシリアル番号に対応する利用サービス管理テーブルにサービス B の ID を追加し、サービス B が利用可能になったことをサーバ 33 に通知する（ステップ S 18）。そして、サーバ 33 は、ユーザ情報管理テーブル 37 に、共通証明書のシリアル番号を記録して（ステップ S 19）、処理を終了する。

【0051】

ステップ S 13 において、共通証明書のシリアル番号がユーザ情報管理テーブル 37 に登録されていれば、次に、サービス B の利用を禁止するか否かをユーザ 31 に問い合わせる（ステップ S 20-1）。そして、ユーザ 31 が利用禁止を希望しなければ、そのまま処理を終了する。

【0052】

ユーザ 31 が利用禁止を希望すれば、次に、提示された共通証明書のシリアル番号をユーザ情報管理テーブル 37 から削除し（ステップ S 20-2）、その共通証明書の利用可能サービスからサービス B を抹消するように、認証局 34 に依頼する（ステップ S 20-3）。

【0053】

これを受けて、認証局 34 は、対応する利用サービス管理テーブルからサービス B のサービス ID を削除し、サービス B を抹消したことをサーバ 33 に通知する（ステップ S 20-4）。そして、サーバ 33 は、サービス B の利用が禁止されたことをユーザ 31 に通知して、処理を終了する。

【0054】

以上の説明では、証明書管理テーブルと利用サービス管理テーブルを別々に設けているが、これらのテーブルの情報を1つのテーブルにまとめて格納してもよい。

【0055】

次に、図10および図11を参照しながら、インターネット上の会員制サービスであるniftyにおいて、上述した認証システムを適用した例を説明する。

現在、niftyと連動して各種分野のポータルサイト(portal site)を構築し、多くの企業のサービスを提供する動きが見られる。ポータルサイトは、インターネットの入口となる巨大なWebサイトであり、様々なサービスサイトへのリンクを保持している。しかし、複数の独立したサービスをポータルサイトに集中させると、認証の煩雑さが大きな問題となる。これは、niftyに限らず、どのポータルサイトでも起こり得る問題である。このような場合に、上述した共通認証の仕組みを用いれば、複数のサービスによる認証が簡便化される。

【0056】

図10は、金融関連サービスを提供するポータルサイトFinance@niftyを含むサービスシステムの構成図である。図10のサービスシステムは、インターネット41、認証局のサーバ42、@nifty会員サービスのサーバ43、銀行のサーバ44、クレジット会社のサーバ45、保険会社のサーバ46、インターネットショップのサーバ47、電力会社のサーバ48、ガス会社のサーバ49、およびユーザ端末50を含む。

【0057】

ここで、@nifty、銀行、クレジット会社、保険会社、インターネットショップ、電力会社、およびガス会社は、それぞれ、独立した会員制サービスを提供する事業体に相当する。

【0058】

認証局のサーバ42は、証明書管理DB35、証明書管理部51、およびサービス管理DB52を備える。証明書管理DB35は、各共通証明書の証明書管理テーブルおよび利用サービス管理テーブルを格納し、証明書管理部51は、証明書管理DB35を用いて、共通証明書の発行、チェック、失効等の処理を行う。

また、サービス管理DB52は、各サービスに関する情報を格納し、証明書管理部51は、サービス管理DB52を用いて、各サービスの入会審査に関する処理を行う。

【0059】

また、@nifty会員サービスのサーバ43は、会員画面制御部61、請求管理部62、ユーザ管理DB63、画面レイアウトDB64、および請求情報DB65を備える。ユーザ管理DB63は、各ユーザのユーザ情報管理テーブルを格納し、画面レイアウトDB64は、会員サービス画面のデータを格納し、請求情報DB65は、サーバ47、48、49等から収集される請求金額のデータを格納する。

【0060】

会員画面制御部61は、ユーザ管理DB63および画面レイアウトDB64を用いて、ユーザ端末50上の画面表示を制御し、請求管理部62は、請求情報DB65を用いて、請求金額の表示を制御する。

【0061】

例えば、ユーザ端末50の画面に表示されたFinance@niftyのページ71は、会員サービス81および証明書82の項目を含む。そして、ユーザがこれらの項目を指定すると、ユーザ端末50が保持している共通証明書が自動的にサーバ43に送られ、認証が行われて、会員メニューのページ72が表示される。このページ72には、公共料金決済サービス83、明細表示サービス84、転居手続きサービス85、および会員設定86の項目が含まれている。

【0062】

このうち、ユーザが公共料金決済サービス83を選択すると、共通証明書がサーバ44に送られ、認証が行われて、公共料金決済のページ73が表示される。このページ73には、口座振替申込み87、インターネット個別払い88、および銀行決済申込み89の項目が含まれている。

【0063】

また、ユーザが明細表示サービス84を選択すると、ユーザの金融情報の明細を示すページ74が表示される。このとき、必要に応じて、共通証明書がサーバ

4 4、4 5 等にも送られ、認証が行われる。

【 0 0 6 4 】

このページ 7 4 のレイアウトデータは、会員画面制御部 6 1 から提供され、請求金額のデータは、請求管理部 6 2 から提供される。さらに、銀行口座の残高データは、銀行のサーバ 4 4 から提供され、クレジットカードの請求明細のデータは、クレジット会社のサーバ 4 5 から提供される。

【 0 0 6 5 】

図 1 1 は、図 1 0 のサービスシステムにおいて、ユーザが明細表示サービス 8 4 を利用する場合のシーケンスを示している。この処理においては、以下のシーケンスに従って、@ n i f t y、銀行、クレジット会社等の複数の事業体のサービスが複合的に提供される。

【 0 0 6 6 】

P 3 1 : ユーザは、共通証明書を提示して、ユーザ端末 5 0 から F i n a n c e @ n i f t y のサイトにアクセスする。

P 3 2 : @ n i f t y のサーバ 4 3 は、提示された共通証明書のシリアル番号を、認証局のサーバ 4 2 に通知する。

【 0 0 6 7 】

P 3 3 : サーバ 4 2 は、証明書管理 D B 3 5 の対応する利用サービス管理テーブルを参照し、その共通証明書で @ n i f t y 会員サービスが利用可能であれば、チェック結果として O K を返す。

【 0 0 6 8 】

P 3 4 : サーバ 4 3 は、会員メニュー 7 2 を表示する。

P 3 5 : ユーザは、会員メニュー 7 2 から明細表示サービスを選択する。

P 3 6 : サーバ 4 3 は、共通証明書のシリアル番号を認証局のサーバ 4 2 に通知して、利用可能サービスを問い合わせる。

【 0 0 6 9 】

P 3 7 : サーバ 4 2 は、対応する利用サービス管理テーブルを参照して、通知されたシリアル番号に対応する利用可能サービス I D を取得し、それをサーバ 4 3 に返す。

【 0 0 7 0 】

P 3 8 : サーバ 4 3 は、受け取った各サービス ID に対応する表示領域を含む、画面描画用のレイアウトデータをユーザ端末 5 0 に送る。このレイアウトデータは、HTML (hypertext markup language)、XML (extensible markup language) 等で記述される。

【 0 0 7 1 】

P 3 9 : ユーザ端末 5 0 は、共通証明書を提示して、A 銀行のサーバに明細情報を問い合わせる。

P 4 0 : A 銀行のサーバは、提示された共通証明書のシリアル番号を、認証局のサーバ 4 2 に通知する。

【 0 0 7 2 】

P 4 1 : サーバ 4 2 は、証明書管理 DB 3 5 の対応する利用サービス管理テーブルを参照し、その共通証明書で A 銀行のサービスが利用可能であれば、チェック結果として OK を返す。

【 0 0 7 3 】

P 4 2 : A 銀行のサーバは、ユーザ口座の残高データを、明細情報としてユーザ端末 5 0 に送る。

P 4 3 ~ P 4 6 : B 銀行のサーバも、A 銀行のサーバと同様にして、共通証明書による認証に基づいて、ユーザ口座の残高データをユーザ端末 5 0 に送る。

【 0 0 7 4 】

こうして、ユーザ端末 5 0 の画面に、明細ページ 7 4 が表示される。クレジット会社のサーバ 4 5 や保険会社のサーバ 4 6 も、同様のシーケンスで、明細ページ 7 4 に明細情報を提供することができる。

【 0 0 7 5 】

図 1 0 のサービスシステムによれば、各サービスが別々に保持している口座残高や請求金額等の明細情報を、1 つのレイアウト画面上に統合して表示することができ、複数のサービスの横断利用が可能になる。図 1 0 においては、認証局の機能が各サービスから独立しているが、この機能を @ n i f t y 会員サービスの中に取り込んでもよい。

【 0 0 7 6 】

次に、図 1 2 から図 2 6 までを参照しながら、図 1 0 の認証局のサーバ 4 2 により行われる、入会審査に関する処理について説明する。

サーバ 4 2 のサービス管理 DB 5 2 には、複数のサービスの入会審査基準情報が蓄積され、証明書管理部 5 1 は、それらの入会審査基準情報を参照しながら、加入可能サービス表示処理、入会審査処理、および加入条件シミュレーション処理を行う。

【 0 0 7 7 】

加入可能サービス表示処理では、各サービスの入会審査基準情報に基づき、複数のサービスの中から特定ユーザが利用できるサービスを選別して表示する。入会審査処理では、各サービスのサーバに代わって、入会希望ユーザが既に参加している他のサービスの情報を参照することで、そのユーザの入会審査を行う。加入条件シミュレーション処理では、各サービスの入会審査基準情報に基づいて、新たな入会審査基準のシミュレーションを行う。

【 0 0 7 8 】

図 1 2 は、サービス管理 DB 5 2 に格納されるサービステーブルの例を示しており、図 1 3 は、サービス管理 DB 5 2 に格納される入会判断テーブルの例を示している。これらのテーブルは、サービス毎に生成される。

【 0 0 7 9 】

図 1 2 のサービステーブルには、サービス ID、会社 ID、サービスに対するユーザの加入条件 1 ～ t、サービス分野、サービス名称、サービス概要、加入申込み URL (uniform resource locator)、および加入問い合わせ e メールアドレスが登録されている。このうち、加入条件 1 ～ t が入会審査基準情報に対応し、このサービスの場合は、性別、年齢、年収、勤務先等が加入条件として設けられている。ここでは、4 0 才以下で年収 6 0 0 万円以上の女性がサービスに加入することができる。

【 0 0 8 0 】

また、図 1 3 の入会判断テーブルには、サービス ID と判断基準が登録されている。判断基準は、会社 ID と、その会社が提供しているサービスのサービス I

Dを含む。この入会判断テーブルは、入会希望ユーザによる他の会社のサービス加入状況に基づいて、そのユーザの入会可否を判断するために用いられる。

【 0 0 8 1 】

図 1 3 の判断基準によれば、会社 “ a a a a a ” のサービス “ * * * * B ” および “ * * * * C ” とともに、会社 “ b b b b b ” のいずれかのサービスを利用しているユーザ、または、会社 “ c c c c c ” のサービス “ * * * * D ” を利用しているユーザに対して、入会が許可される。

【 0 0 8 2 】

ただし、サービス I D の内容（番号配列）から会社を特定できる場合は、必ずしも会社 I D を保持する必要はない。また、入会判断テーブルの判断基準を満たさないユーザについては、サービステーブルの加入条件に基づいて、通常の入会審査が行われる。

【 0 0 8 3 】

図 1 4 は、ユーザまたはサービス運用者が認証局のサーバ 4 2 にアクセスしたときに表示されるメニュー画面の例を示している。図 1 4 のメニューには、加入可能サービス表示 9 1、入会審査 9 2、および加入条件シミュレーション 9 3 の項目が含まれている。ユーザが共通証明書を提示して、加入可能サービス表示 9 1 を指定すると、サービス表示処理が行われる。また、サービス運用者が入会審査 9 2 を指定すると、入会審査処理が行われ、加入条件シミュレーション 9 3 を指定すると、加入条件シミュレーション処理が行われる。

【 0 0 8 4 】

ただし、メニュー画面は、加入者用画面とサービス運用者用画面に分類して表示することもあり得る。この場合、ユーザまたはサービス運用者が利用可能な項目のみが画面に表示される。

【 0 0 8 5 】

図 1 5 および図 1 6 は、サーバ 4 2 の証明書管理部 5 1 による加入可能サービス表示処理のフローチャートである。証明書管理部 5 1 は、まず、ユーザから提示された共通証明書のシリアル番号に基づいて、証明書管理 D B 3 5 の対応する利用サービス管理テーブルを参照し、登録されているサービス I D を取得する（

図 1 5 のステップ S 2 1)。

【 0 0 8 6 】

そして、取得したサービス I D の数を判定する (ステップ S 2 2)。これらのサービス I D は、そのユーザが既に加入済みのサービスを表している。サービス I D が複数であれば、サービス管理 D B 5 2 を参照して、それらのサービス I D に対応するサービステーブルから加入条件を抽出し、複数のサービスの加入条件を A N D 処理により合算する (ステップ S 2 3)。そして、得られた条件を加入済みサービスの条件として記録する。また、サービス I D が 1 つの場合は、対応するサービステーブルの加入条件を、加入済みサービスの条件として記録する。

【 0 0 8 7 】

次に、加入済みサービス以外の未加入サービスのサービステーブルの 1 つを呼び出し (ステップ S 2 4)、加入済みサービスの条件を、未加入サービスの対応する条件と比較する (ステップ S 2 5)。加入済みサービスの条件が未加入サービスの条件を満たさなければ、ステップ S 2 4 の処理を繰り返す。

【 0 0 8 8 】

加入済みサービスの条件が未加入サービスの条件を満たせば、次に、呼び出されたサービステーブルに他の加入条件が設定されているか否かをチェックする (ステップ S 2 6)。他の条件が設定されていなければ、すぐに加入可能と判断し、メモリ上のバッファ領域に設けられた、すぐに加入可能なサービスの一覧テーブルに、その未加入サービスの分野、名称、および概要を記録する (ステップ S 2 7)。

【 0 0 8 9 】

次に、未加入サービスのサービステーブルが終了したか否かを判定し、そのようなサービステーブルが残っていれば、ステップ S 2 4 以降の処理を繰り返す。また、ステップ S 2 6 において、他の条件が設定されていれば、条件付きで加入可能と判断し、バッファ領域に設けられた、条件付きで加入可能なサービスの一覧テーブルに、その未加入サービスの分野、名称、概要、および設定されている他の条件を記録する (ステップ S 2 9)。そして、ステップ S 2 8 以降の処理を行う。

【 0 0 9 0 】

そして、ステップ S 2 8 において、未加入サービスのサービステーブルが終了すると、ステップ S 2 7 および S 2 9 で生成された一覧テーブルの内容を、図 1 7 のようなサービス選択画面として、ユーザ端末 5 0 に表示する（ステップ S 3 0）。

【 0 0 9 1 】

図 1 7 のサービス選択画面には、ユーザが現在加入しているサービスと、新たに加入可能なサービスとが表示されている。このうち、新たに加入可能なサービスは、すぐに加入可能なサービスと、条件付きで加入可能なサービスとに分けて表示される。

【 0 0 9 2 】

このようなサービス選択画面において、ユーザがいずれかの未加入サービスを選択すると（図 1 6 のステップ S 3 1）、証明書管理部 5 1 は、対応するサービステーブルを参照して、そのサービスの加入申込み URL を取得し、ユーザ端末 5 0 に送信する（ステップ S 3 2）。これにより、ユーザの画面は選択されたサービスのサイトにジャンプして、加入申込み画面が表示される（ステップ S 3 3）。その後、ユーザは、加入申込み画面の指示に従って、申込みを行う。

【 0 0 9 3 】

ユーザは、加入申込み画面から申込みを行う代わりに、選択したサービスのサイトに加入問い合わせ e メールを送ることもできる。この場合、ステップ S 3 2 および S 3 3 において、証明書管理部 5 1 は、対応するサービステーブルから加入問い合わせ e メールアドレスを取得し、ユーザ端末に表示する。

【 0 0 9 4 】

このような加入可能サービス表示処理によれば、ユーザは、入会審査を受ける前に、加入可能な未加入サービスの一覧を取得することができる。したがって、すべての未加入サービスの入会審査を受けなくても、加入可能サービスを絞り込むことができ、その中から加入サービスを選択することができる。

【 0 0 9 5 】

図 1 8 および図 1 9 は、証明書管理部 5 1 による入会審査処理のフローチャー

トである。まず、証明書管理部 5 1 は、図 2 0 のような条件入力画面を、サービス運用者の端末（例えば、サービスを提供するサーバ）に表示し、入会審査判断情報の入力を促す（図 1 8 のステップ S 4 1）。これに応じて、サービス運用者は、入会希望ユーザの共通証明書のシリアル番号と、そのユーザが希望しているサービスのサービス ID を入力する。

【 0 0 9 6 】

次に、証明書管理部 5 1 は、サービス管理 DB 5 2 を参照して、入力されたサービス ID に対応する入会判断テーブルを検索する（ステップ S 4 2）。ここで、サービス事業体があらかじめ入会判断テーブルを登録していれば、その入会判断テーブルを呼び出す。

【 0 0 9 7 】

次に、証明書管理 DB 3 5 を参照して、入力されたシリアル番号に対応する利用サービス管理テーブルを検索する（ステップ S 4 3）。そして、対応する利用サービス管理テーブルがなければ、ユーザが見つからないこと、または、ユーザが他のサービスを利用していないことを通知するメッセージを表示して（ステップ S 4 4）、処理を終了する。

【 0 0 9 8 】

また、対応する利用サービス管理テーブルがあれば、それを呼び出し、次に、利用サービス管理テーブルに登録されたサービス ID と入会判断テーブルの判断基準とを比較する（ステップ S 4 5）。そして、サービス ID が入会判断テーブルの判断基準を満たせば、入会資格ありと判断し、図 2 1 のような判断結果画面を表示して（ステップ S 4 6）、処理を終了する。

【 0 0 9 9 】

サービス事業体があらかじめ入会判断テーブルを登録していなければ、ステップ S 4 2 において、対応する入会判断テーブルが見つからないので、図 1 9 の処理が行われる。また、ステップ S 4 5 において、サービス ID が判断基準を満たさない場合も、図 1 9 の処理が行われる。

【 0 1 0 0 】

図 1 9 のステップ S 4 7 および S 4 8 の処理は、図 1 8 のステップ S 4 3 およ

び S 4 4 の処理と同様である。また、図 1 9 のステップ S 4 9 および S 5 0 の処理は、図 1 5 のステップ S 2 2 および S 2 3 の処理と同様である。

【0 1 0 1】

ステップ S 4 9 および S 5 0 の処理により、加入済みサービスの条件が記録されると、次に、サービス運用者から提供されたサービス ID に対応する対象サービスのサービステーブルを呼び出し（図 1 9 のステップ S 5 1）、加入済みサービスの条件を、対象サービスの対応する条件と比較する（ステップ S 5 2）。

【0 1 0 2】

加入済みサービスの条件が対象サービスの条件を満たさなければ、入会資格なしと判断し、図 2 2 のような判断結果画面を表示して（ステップ S 5 3）、処理を終了する。図 2 2 の画面には、入会資格があるとは判断できないことを通知するメッセージが表示されている。さらに、入会審査を続行するにはユーザから個人情報入手する必要があることを通知するメッセージを追加してもよい。

【0 1 0 3】

加入済みサービスの条件が対象サービスの条件を満たせば、次に、呼び出されたサービステーブルに他の加入条件が設定されているか否かをチェックする（ステップ S 5 4）。他の条件が設定されていなければ、入会資格ありと判断し、図 2 1 のような判断結果画面を表示して（ステップ S 5 5）、処理を終了する。

【0 1 0 4】

他の条件が設定されていれば、その条件を取得する（ステップ S 5 6）。そして、条件付きで入会資格ありと判断し、図 2 3 のような判断結果画面を表示して（ステップ S 5 7）、処理を終了する。図 2 3 の画面には、設定された他の条件が、明確にすべき追加条件として表示されている。

【0 1 0 5】

このように、認証局がユーザの利用可能サービスを集中管理し、そのユーザが新たなサービスに加入するときに、サービス事業体に代わって入会審査を行うことで、入会審査のためのサービス運用者の負荷が軽減される。例えば、銀行サービスと保険サービスの利用資格があるユーザには、クレジットサービスの従来の入会審査を省略することが可能になる。

【0106】

図24は、証明書管理部51による加入条件シミュレーション処理のフローチャートである。まず、証明書管理部51は、図25のようなシミュレーション画面を、サービス運用者の端末に表示し、シミュレーション対象となる加入条件の入力を促す（ステップS61）。これに応じて、サービス運用者は、性別、年令、年収等の条件を入力し、試算ボタン101を押す。

【0107】

次に、証明書管理部51は、メモリ上のバッファ領域に、入力された加入条件を有する仮想サービステーブルを作成し（ステップS62）、サービス管理DB52から既存のサービステーブルの1つを呼び出す（ステップS63）。そして、仮想サービステーブルの条件を、既存のサービステーブルの対応する条件と比較する（ステップS64）。

【0108】

仮想サービステーブルの条件が既存のサービステーブルの条件を満たさなければ、ステップS63の処理を繰り返す。仮想サービステーブルの条件が既存のサービステーブルの条件を満たせば、次に、既存のサービステーブルに他の加入条件が設定されているか否かをチェックする（ステップS65）。他の条件が設定されていれば、ステップS63以降の処理を繰り返す。

【0109】

他の条件が設定されていなければ、証明書管理DB35を参照して、既存のサービステーブルに記録されたサービスIDを登録している利用サービス管理テーブルを検索する。そして、そのような利用サービス管理テーブルの1つから共通証明書のシリアル番号を取得し（ステップS66）、メモリ上のバッファ領域に設けられた、図26のような加入者カウントテーブルに、そのシリアル番号が登録されているか否かをチェックする（ステップS67）。

【0110】

シリアル番号が既に登録されていれば、ステップS66以降の処理を繰り返し、それがまだ登録されていなければ、加入者カウントテーブルに追加する。次に、既存のサービステーブルが終了したか否かをチェックし（ステップS69）、

既存のサービステーブルが残っていれば、ステップ S 6 3 以降の処理を繰り返す。

【 0 1 1 1 】

そして、既存のサービステーブルが終了すると、次に、加入者カウントテーブルに登録されたシリアル番号の数をカウントし（ステップ S 7 0）、その結果をシミュレーション画面に表示して（ステップ S 7 1）、処理を終了する。

【 0 1 1 2 】

図 2 5 の画面では、カウントされたシリアル番号の数が、入力された条件に対する加入可能ユーザの数として表示されており、発行済みの共通証明書の総数に対する加入可能ユーザの割合が、百分率として表示されている。サービス運用者は、入力条件を変更しながらシミュレーションを繰り返すことで、所望のユーザ数に対応する加入条件を決定することができる。ただし、加入可能ユーザの数と割合のうち、一方のみを画面に表示することもあり得る。

【 0 1 1 3 】

このような加入条件シミュレーション処理によれば、サービス運用者は、新たなサービスを開始するとき、あるいは、既存のサービスの加入条件を変更するときに、入会審査に用いる加入条件と会員数の関係をシミュレートしながら、加入条件を効率良く設定することができる。したがって、サービス運用者の負荷が軽減される。

【 0 1 1 4 】

図 1 0 のサーバ 4 2 ～ 4 9 およびユーザ端末 5 0 は、例えば、図 2 7 に示すような情報処理装置（コンピュータ）を用いて構成することができる。図 2 7 の情報処理装置は、CPU（中央処理装置）1 1 1、メモリ 1 1 2、入力装置 1 1 3、出力装置 1 1 4、外部記憶装置 1 1 5、媒体駆動装置 1 1 6、およびネットワーク接続装置 1 1 7 を備え、それらはバス 1 1 8 により互いに接続されている。

【 0 1 1 5 】

メモリ 1 1 2 は、例えば、ROM（read only memory）、RAM（random access memory）等を含み、処理に用いられるプログラムとデータを格納する。CPU 1 1 1 は、メモリ 1 1 2 を利用してプログラムを実行することにより、必要な

処理を行う。

【0116】

例えば、図10の証明書管理部51、会員画面制御部61、および請求管理部62は、プログラムにより記述されたソフトウェアコンポーネントとしてメモリ112に格納される。

【0117】

入力装置113は、例えば、キーボード、ポインティングデバイス、タッチパネル等であり、オペレータ（サービス運用者またはユーザ）からの指示や情報の入力に用いられる。出力装置114は、例えば、ディスプレイ、プリンタ、スピーカ等であり、オペレータへの問い合わせや処理結果の出力に用いられる。

【0118】

外部記憶装置115は、例えば、磁気ディスク装置、光ディスク装置、光磁気ディスク（magneto-optical disk）装置、テープ装置等である。情報処理装置は、この外部記憶装置115に、上述のプログラムとデータを保存しておき、必要に応じて、それらをメモリ112にロードして使用する。また、外部記憶装置115は、図10の証明書管理DB35、サービス管理DB52、ユーザ管理DB63、画面レイアウトDB64、および請求情報DB65としても利用される。

【0119】

媒体駆動装置116は、可搬記録媒体119を駆動し、その記録内容にアクセスする。可搬記録媒体119としては、メモリカード、フロッピーディスク、CD-ROM（compact disk read only memory）、光ディスク、光磁気ディスク等、任意のコンピュータ読み取り可能な記録媒体が用いられる。オペレータは、この可搬記録媒体119に上述のプログラムとデータを格納しておき、必要に応じて、それらをメモリ112にロードして使用する。

【0120】

ネットワーク接続装置117は、インターネット41等の任意の通信ネットワークに接続され、通信に伴うデータ変換を行う。また、情報処理装置は、上述のプログラムとデータをネットワーク接続装置117を介して他の装置から受け取り、必要に応じて、それらをメモリ112にロードして使用する。

【 0 1 2 1 】

図 2 8 は、図 2 7 の情報処理装置にプログラムとデータを供給することのできるコンピュータ読み取り可能な記録媒体を示している。可搬記録媒体 1 1 9 や外部のデータベース 1 2 0 に保存されたプログラムとデータは、メモリ 1 1 2 にロードされる。そして、CPU 1 1 1 は、そのデータを用いてそのプログラムを実行し、必要な処理を行う。

【 0 1 2 2 】

以上説明した実施形態においては、ITU-T の仕様 X. 5 0 9 に基づくデジタル証明書を認証情報として用いているが、必要に応じて、他の仕様の証明書情報を用いてもよい。

【 0 1 2 3 】

【発明の効果】

本発明によれば、ユーザが複数の会員制サービスから加入サービスを選択する際、加入可能なサービスを効率良く絞り込むことができる。また、サービス運用者による入会審査や加入条件設定の作業が効率化される。したがって、入会審査に関する処理において、ユーザおよびサービス運用者の負荷が軽減される。

【図面の簡単な説明】

【図 1】

本発明の処理システムの原理図である。

【図 2】

証明書の発行と審査を示す図である。

【図 3】

証明書の失効を示す図である。

【図 4】

証明書による認証を示す図である。

【図 5】

証明書管理テーブルを示す図である。

【図 6】

利用サービス管理テーブルを示す図である。

【図 7】

ユーザ情報管理テーブルを示す図である。

【図 8】

証明書の発行／失効処理のフローチャートである。

【図 9】

証明書の審査処理のフローチャートである。

【図 1 0】

サービスシステムの構成図である。

【図 1 1】

複数サービスの利用例を示す図である。

【図 1 2】

サービステーブルを示す図である。

【図 1 3】

入会判断テーブルを示す図である。

【図 1 4】

認証局のメニューを示す図である。

【図 1 5】

サービス表示処理のフローチャート（その 1）である。

【図 1 6】

サービス表示処理のフローチャート（その 2）である。

【図 1 7】

サービス選択画面を示す図である。

【図 1 8】

入会審査処理のフローチャート（その 1）である。

【図 1 9】

入会審査処理のフローチャート（その 2）である。

【図 2 0】

条件入力画面を示す図である。

【図 2 1】

第 1 の判断結果画面を示す図である。

【図 2 2】

第 2 の判断結果画面を示す図である。

【図 2 3】

第 3 の判断結果画面を示す図である。

【図 2 4】

シミュレーション処理のフローチャートである。

【図 2 5】

シミュレーション画面を示す図である。

【図 2 6】

加入者カウントテーブルを示す図である。

【図 2 7】

情報処理装置の構成図である。

【図 2 8】

記録媒体を示す図である。

【図 2 9】

従来のサービスシステムを示す図である。

【符号の説明】

- 1 1、3 1 ユーザ
- 1 2、3 2 サービス A のサーバ
- 1 3、1 5 ユーザ管理 D B
- 1 4、3 3 サービス B のサーバ
- 2 1 格納手段
- 2 2 選別手段
- 2 3 提示手段
- 2 4 判定手段
- 2 5 判断手段
- 2 6 設定手段
- 2 7 シミュレーション手段

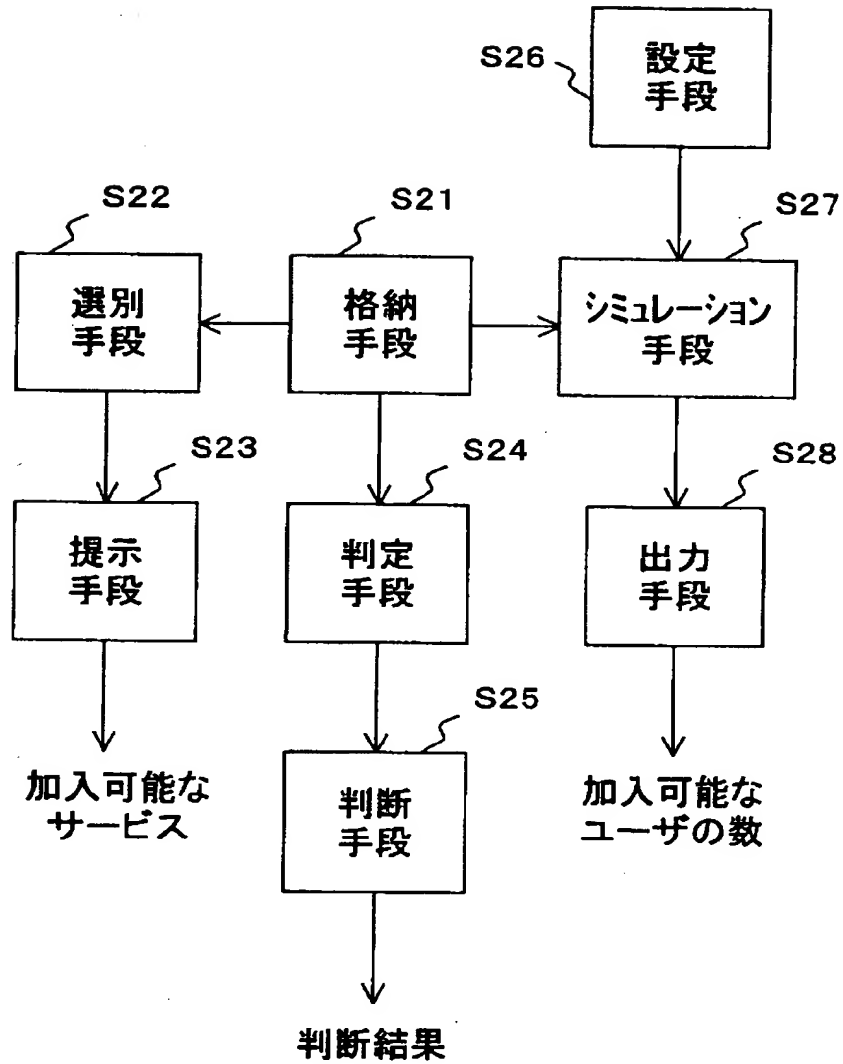
- 2 8 出力手段
- 3 4 認証局
- 3 5 証明書管理 D B
- 3 6、3 7 ユーザ情報管理テーブル
- 4 1 インターネット
- 4 2 認証局のサーバ
- 4 3 @ n i f t y 会員サービスのサーバ
- 4 4 銀行のサーバ
- 4 5 クレジット会社のサーバ
- 4 6 保険会社のサーバ
- 4 7 インターネットショップのサーバ
- 4 8 電力会社のサーバ
- 4 9 ガス会社のサーバ
- 5 0 ユーザ端末
- 5 1 証明書管理部
- 5 2 サービス管理 D B
- 6 1 会員画面制御部
- 6 2 請求管理部
- 6 3 ユーザ管理 D B
- 6 4 画面レイアウト D B
- 6 5 請求情報 D B
- 7 1 f i n a n c e @ n i f t y のページ
- 7 2 会員メニューのページ
- 7 3 公共料金決済のページ
- 7 4 明細ページ
- 8 3 公共料金決済サービス
- 8 4 明細表示サービス
- 8 5 転居手続きサービス
- 8 6 会員設定

- 8 7 口座振替申込み
- 8 8 インターネット個別払い
- 8 9 銀行決済申込み
- 9 1 加入可能サービス表示
- 9 2 入会審査
- 9 3 加入条件シミュレーション
- 1 0 1 試算
- 1 1 1 C P U
- 1 1 2 メモリ
- 1 1 3 入力装置
- 1 1 4 出力装置
- 1 1 5 外部記憶装置
- 1 1 6 媒体駆動装置
- 1 1 7 ネットワーク接続装置
- 1 1 8 バス
- 1 1 9 可搬記録媒体
- 1 2 0 データベース

【書類名】 図面

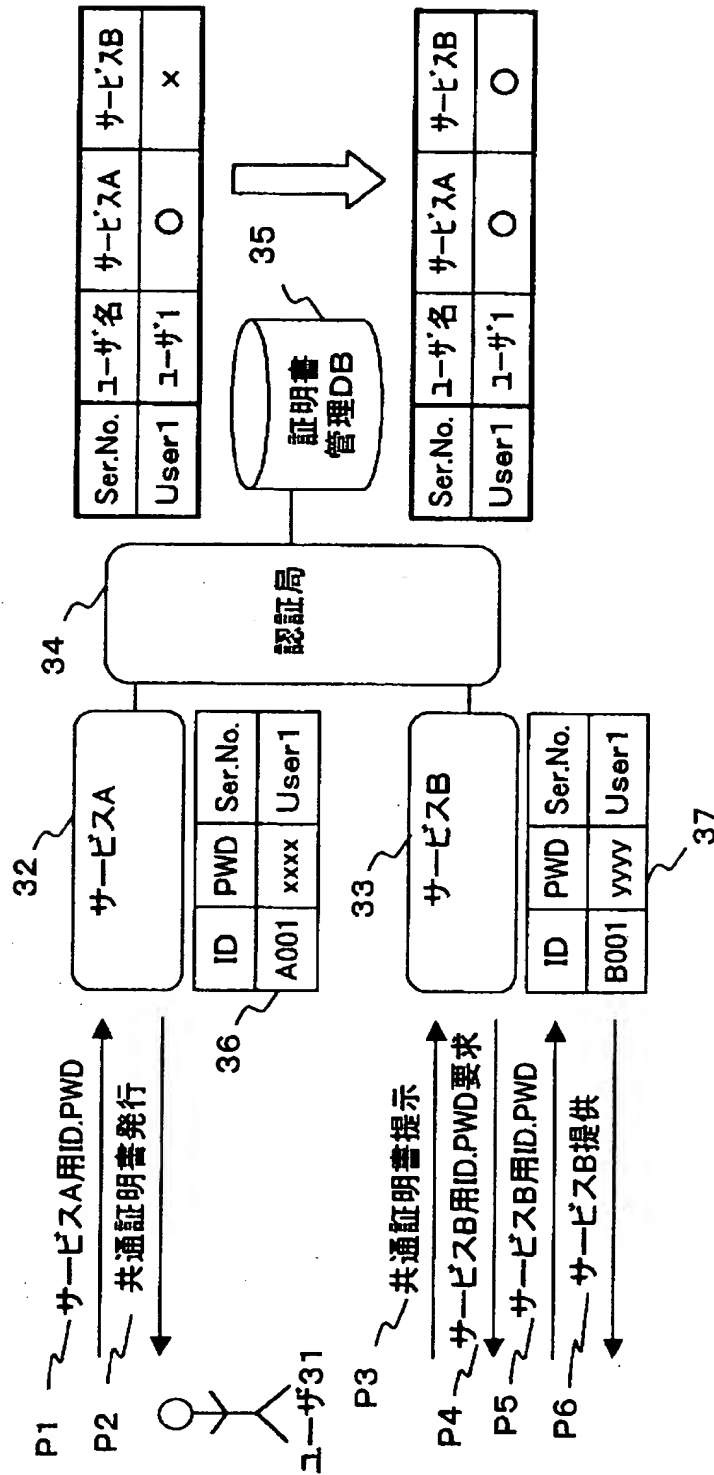
【図 1】

本 発 明 の 原 理 図



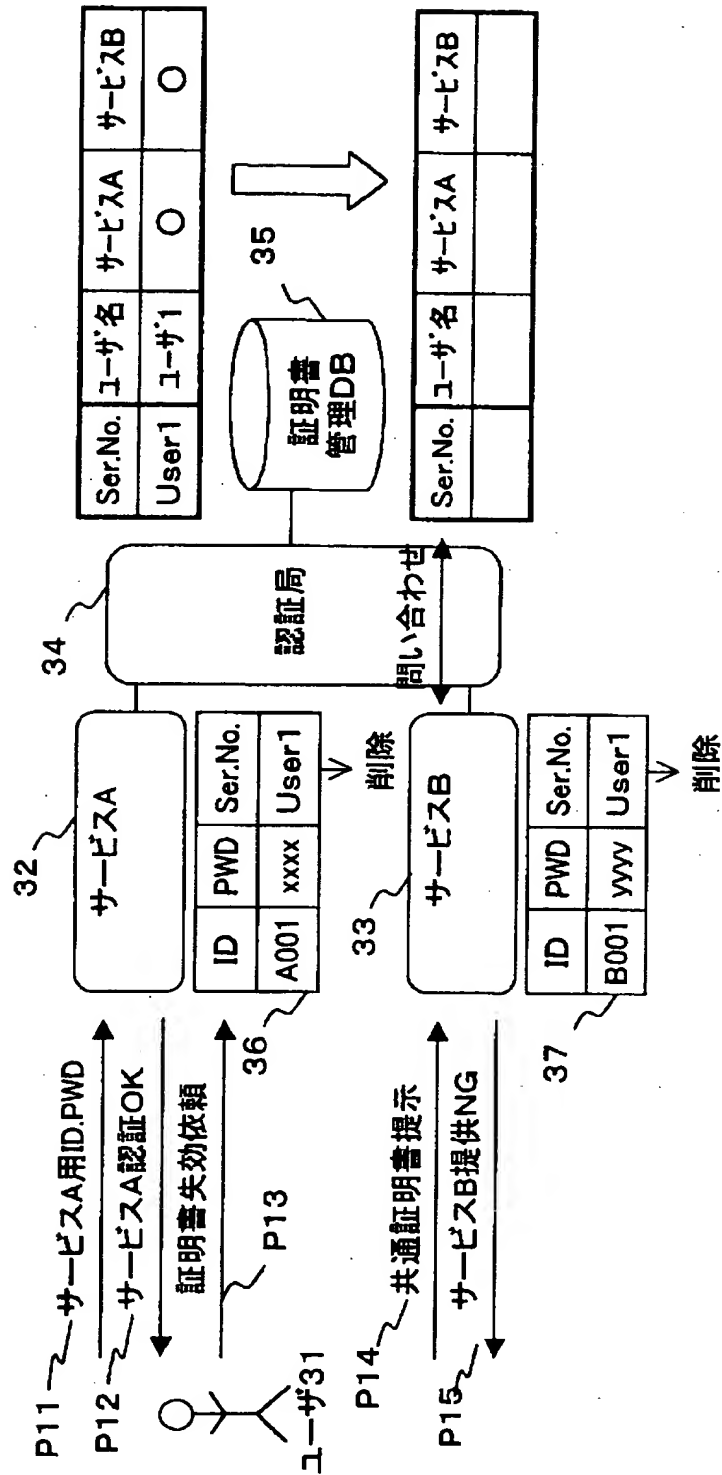
【図 2】

証明書の発行と審査を示す図



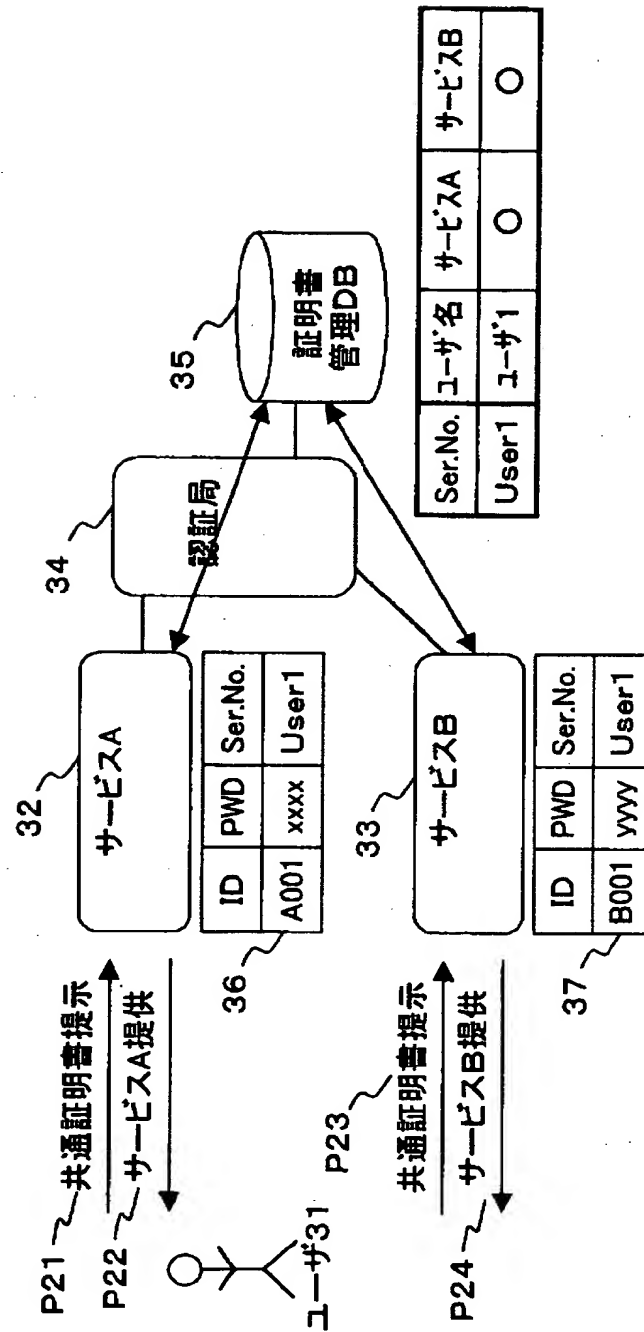
【図 3】

証 明 書 の 失 効 を 示 す 図



【図 4】

証明書による認証を示す図



【図 5】

証 明 書 管 理 テ ー ブ ル を 示 す 図

証明書 Ser. No.	User0001
氏名	富士通太郎
住所	東京都大田区
eメールアドレス	xxx@xxx.jp

【図 6】

利 用 サ ー ビ ス 管 理 テ ー ブ ル を 示 す 図

証明書 Ser. No.	User0001
利用可能サービスID	Service A Service B

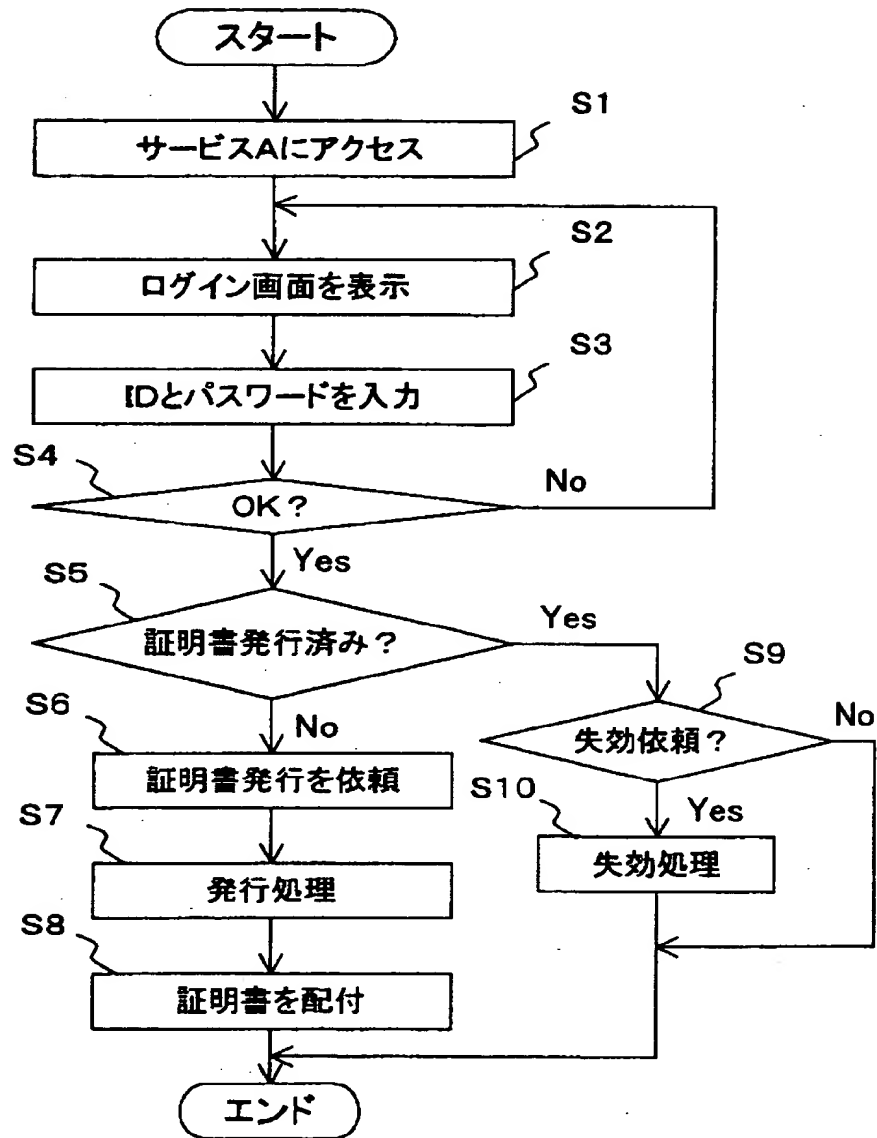
【図 7】

ユーザ情報管理テーブルを示す図

ユーザID	AAA00000
パスワード	XXXXXXXXX
氏名	富士通太郎
住所	東京都大田区
証明書Ser. No.	User0001

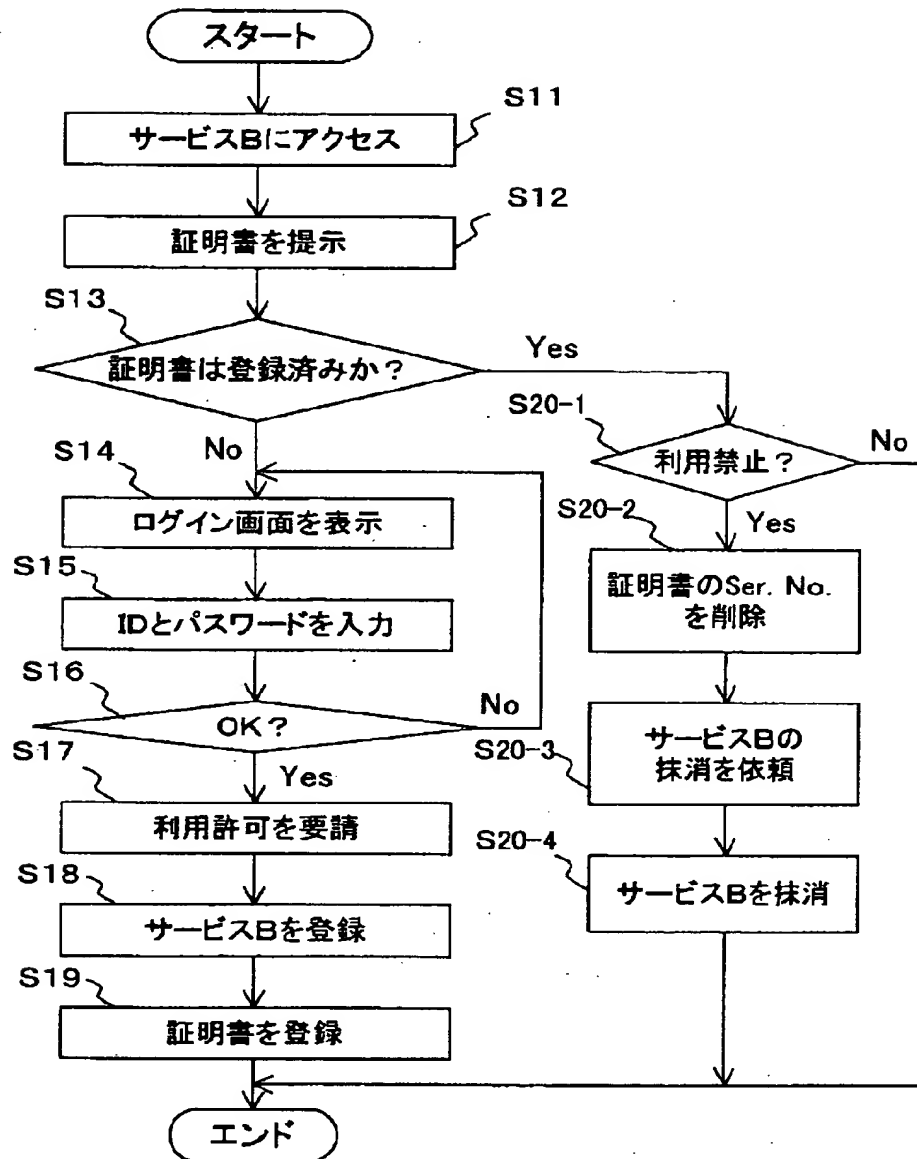
【図8】

証明書の発行／失効処理のフローチャート



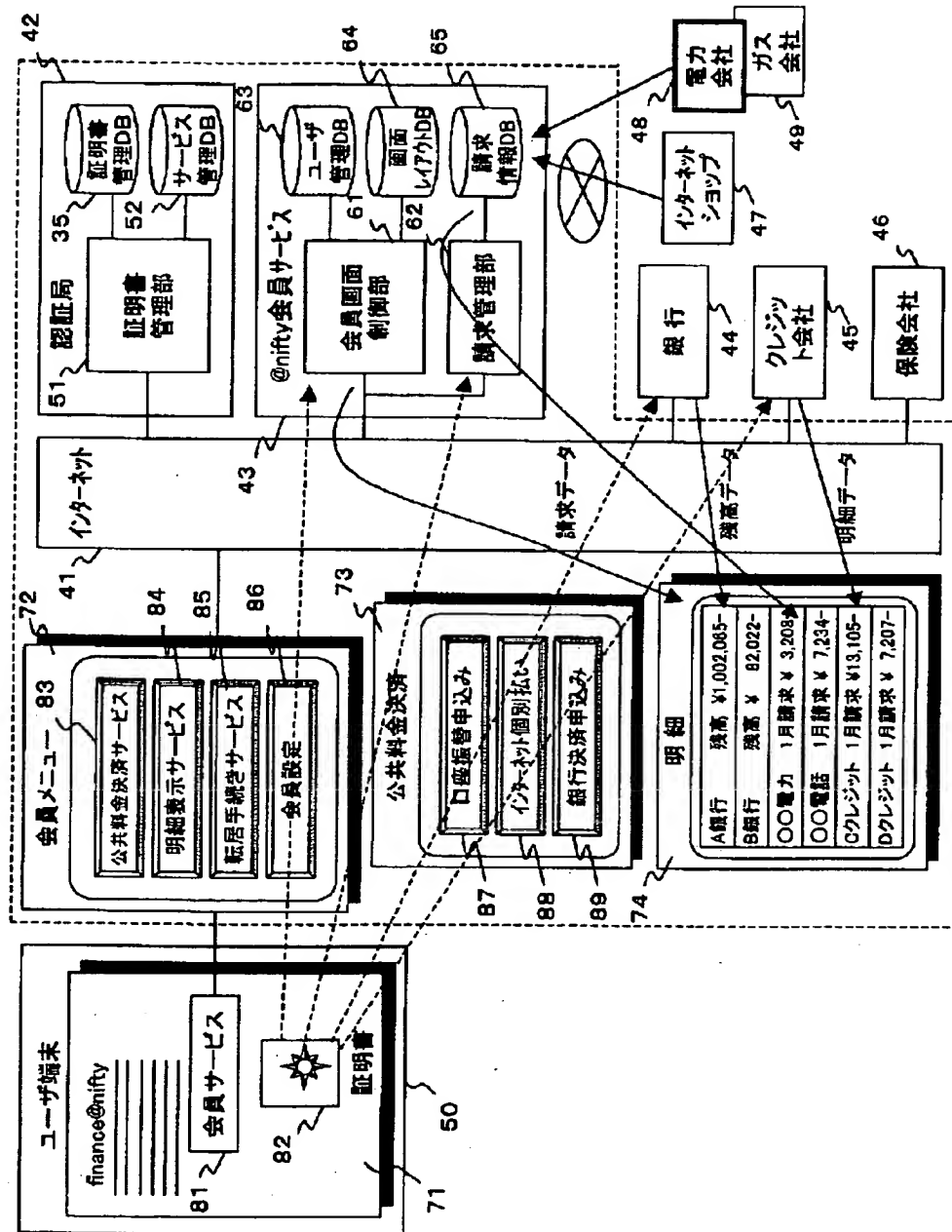
【図9】

証明書の審査処理のフローチャート



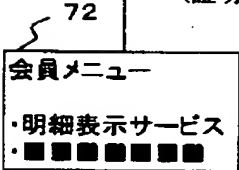
【図10】

サービスシステムの構成図



3. *Chlorophyll a* and *Chlorophyll b* contents were determined by spectrophotometry using the method of Lichtenthaler and Whaley (1987).

複数サービスの利用例を示す図



【図12】

サービステーブルを示す図

サービスID	Service A
会社ID	aaaaa
条件1 性別	<input type="checkbox"/> 男 <input checked="" type="checkbox"/> 女 <input type="checkbox"/> 不問
条件2 年齢	<input type="text" value="40"/> 才 <input type="text" value="以下"/>
条件3 年収	<input type="text" value="600"/> 万円 <input type="text" value="以上"/>
条件4 勤務地	~~~~~
⋮	⋮
条件t 勤務地	~~~~~
サービス分野	~~~~~
サービス名称	~~~~~
サービス概要	~~~~~
加入申込みURL	~~~~~
加入問い合わせeメール	~~~~~

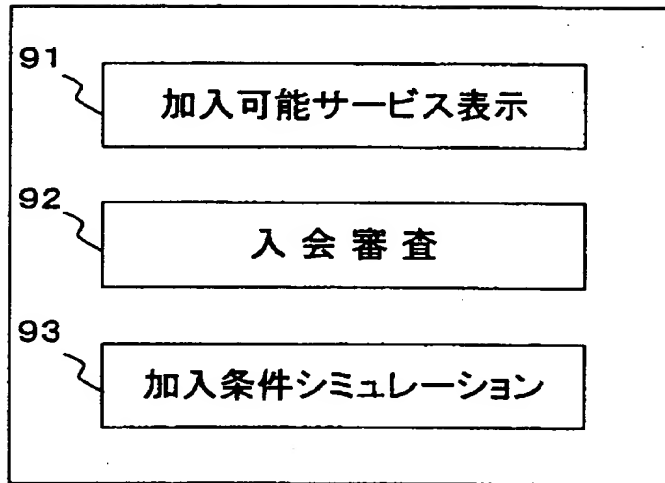
【図 1 3】

入 会 判 断 テ ー ブ ル を 示 す 図

サービスID		Service A
And check	判 断 基 準	
	会社ID	サービスID
	aaaaa	* * * * B, * * * * C,
■	bbbbbb	
	ccccc	* * * * D

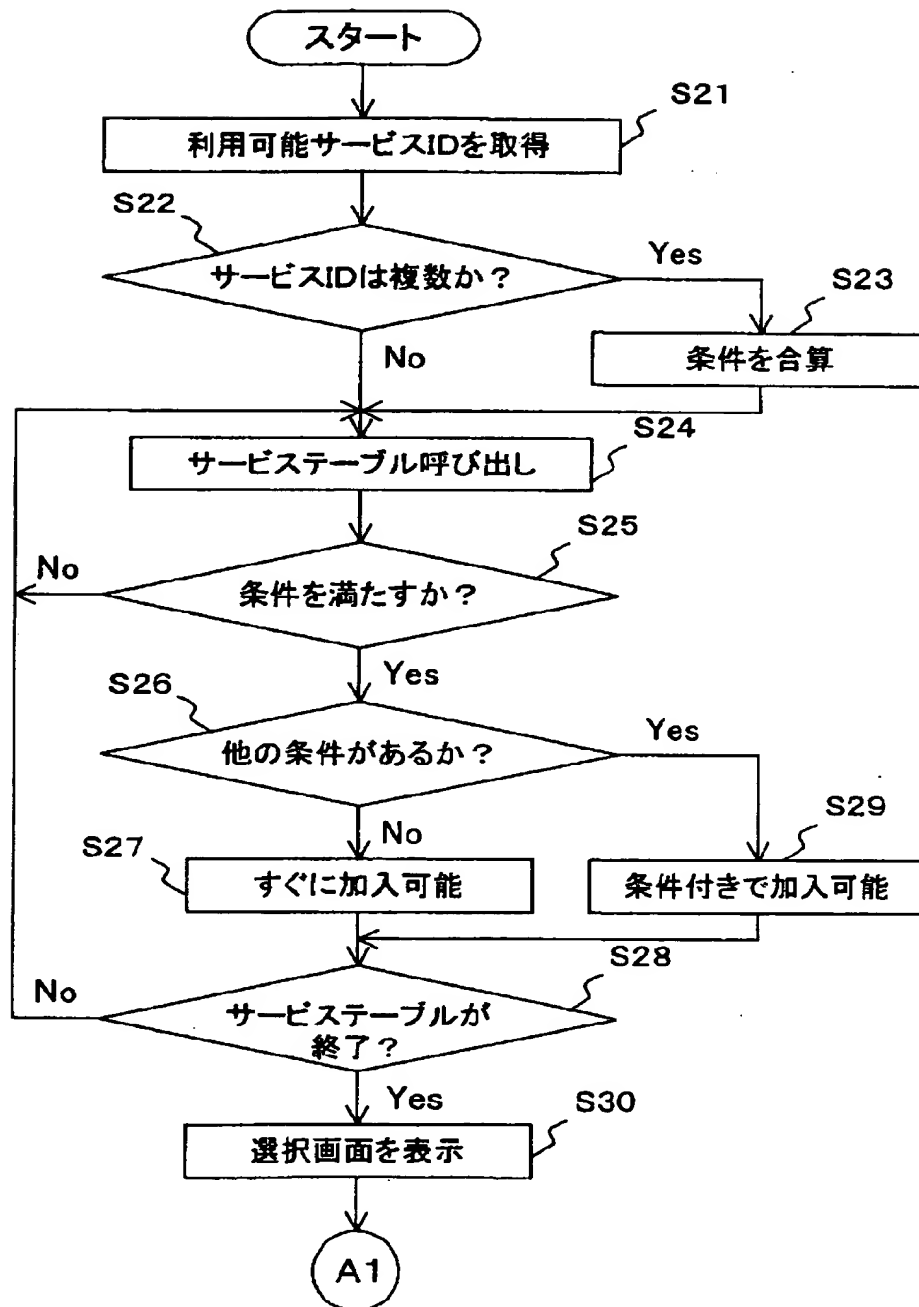
【図 1 4】

認 証 局 の メ ニ ュ ー を 示 す 図



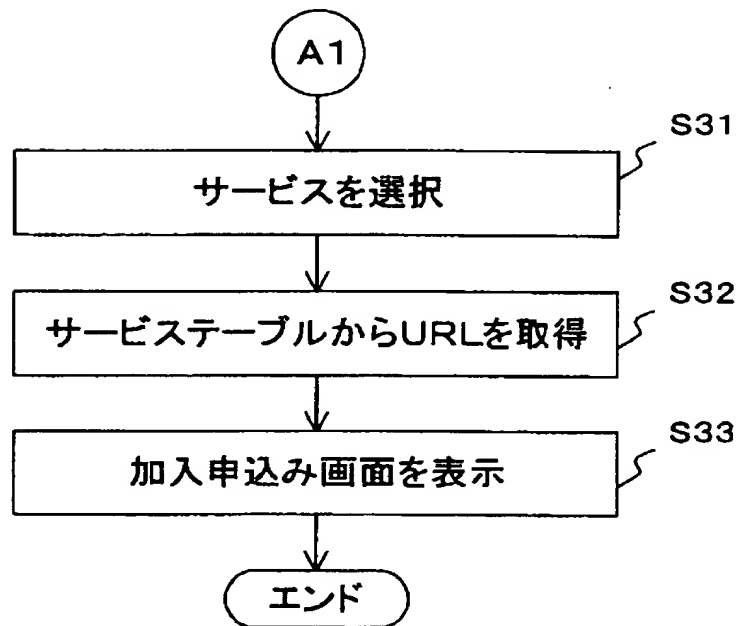
【図 15】

サービス表示処理のフローチャート(その1)



【図 1 6】

サービス表示処理の
フローチャート(その2)



【図 17】

サービス選択画面を示す図

あなたが共通認証システムで加入できるサービス

● 現在あなたが加入しているサービス

1. ○○○ サービス 利用年数 ○○年
 2. ××× サービス 利用年数 ○○年

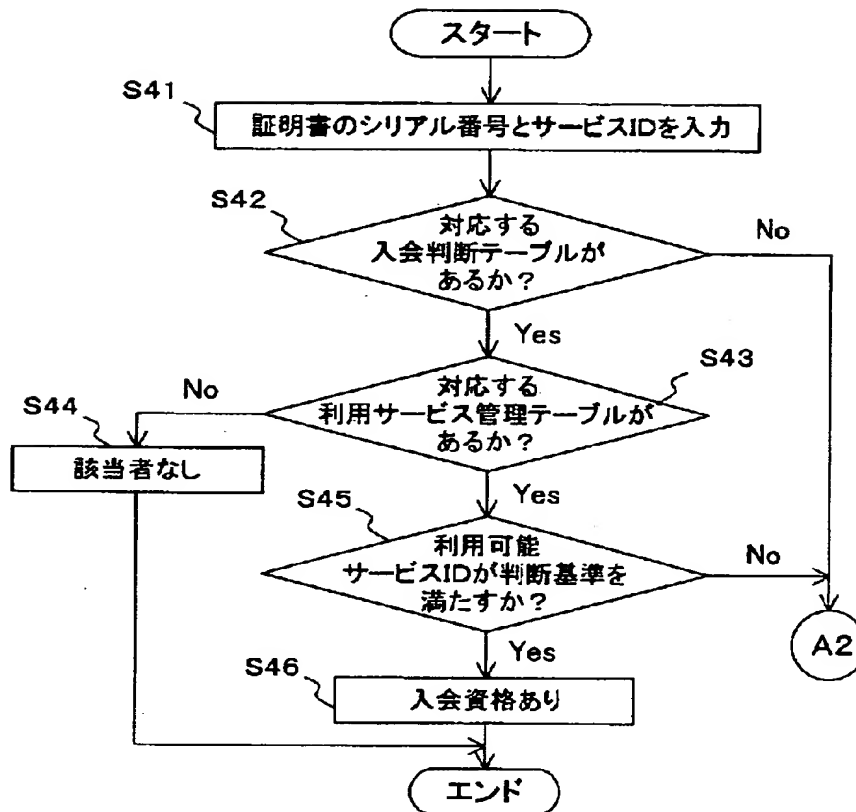
● 新たにあなたが加入できるサービス

すぐに 加入可能	1.	サービス分野	サービス名	サービス概要
	2.	_____	_____	_____
	3.	_____	_____	_____
	3.	_____	_____	_____

条件 付きで 加入可能	1.	サービス分野	サービス名	サービス概要	条 件
	2.	_____	_____	_____	_____
	2.	_____	_____	_____	_____

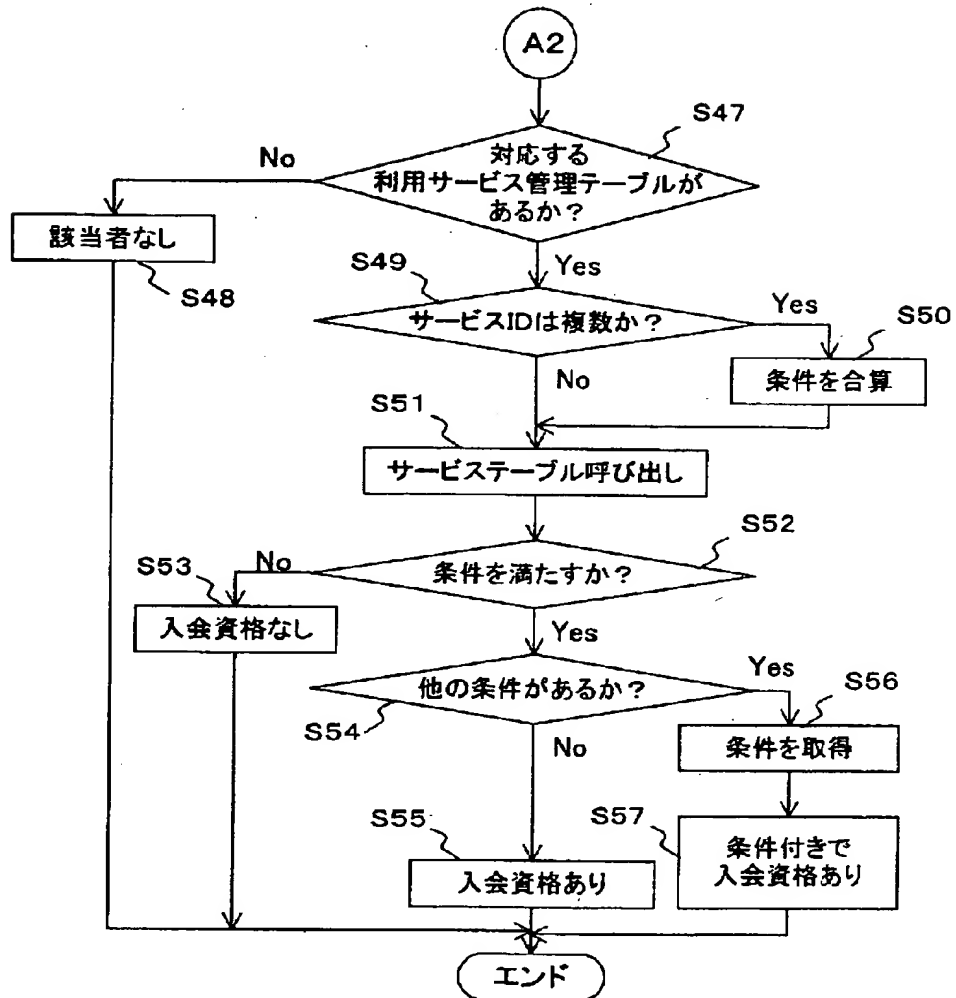
【図18】

入会審査処理のフローチャート(その1)



【図19】

入会審査処理のフローチャート(その2)



【図20】

条件入力画面を示す図

入会審査判断情報

共通認証を利用している利用者が、貴社サービスに入会できるかどうか判断します。

入会希望者の証明書Ser. No.	User0001
入会希望の貴社サービスID	Service A

【図21】

第1の判断結果画面を示す図

入会審査判断 結果 ☒

証明書Ser. No. の利用者は、

貴社サービス ☒ サービス ☐ Service A

に入会できる条件を有しています。

【図22】

第2の判断結果画面を示す図

入会審査判断 結果

×

証明書Ser. No.

User0001

の利用者は、

貴社サービス

○サービス

Service A

の入会資格があるとは判断できません。

【図23】

第3の判断結果画面を示す図

入会審査判断 結果

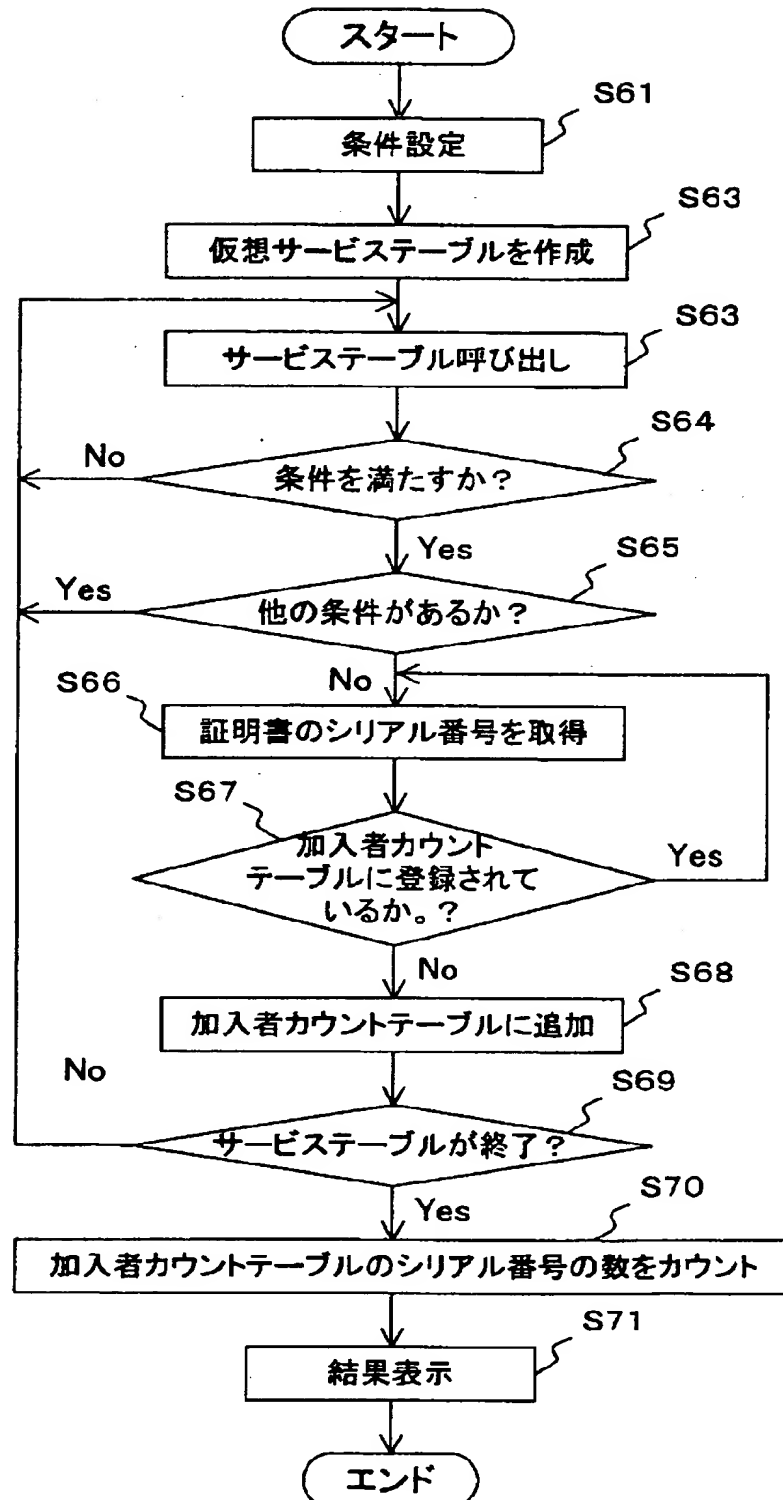
証明書Ser. No. の利用者は、

貴社サービス

を利用する場合、次の条件がよければOK。

【図24】

シミュレーション処理のフローチャート



【図25】

シミュレーション画面を示す図

貴社の加入条件を入力して下さい。

性別 ▼	1.男 2.女 3.不問
性別 ▼	
年齢 ▼	
年収 ▼	
⋮	⋮

条件を設定したら次のボタンを押して下さい。

101 試算

上記設定の条件では %の共通認証

人

利用者が加入できることになります。

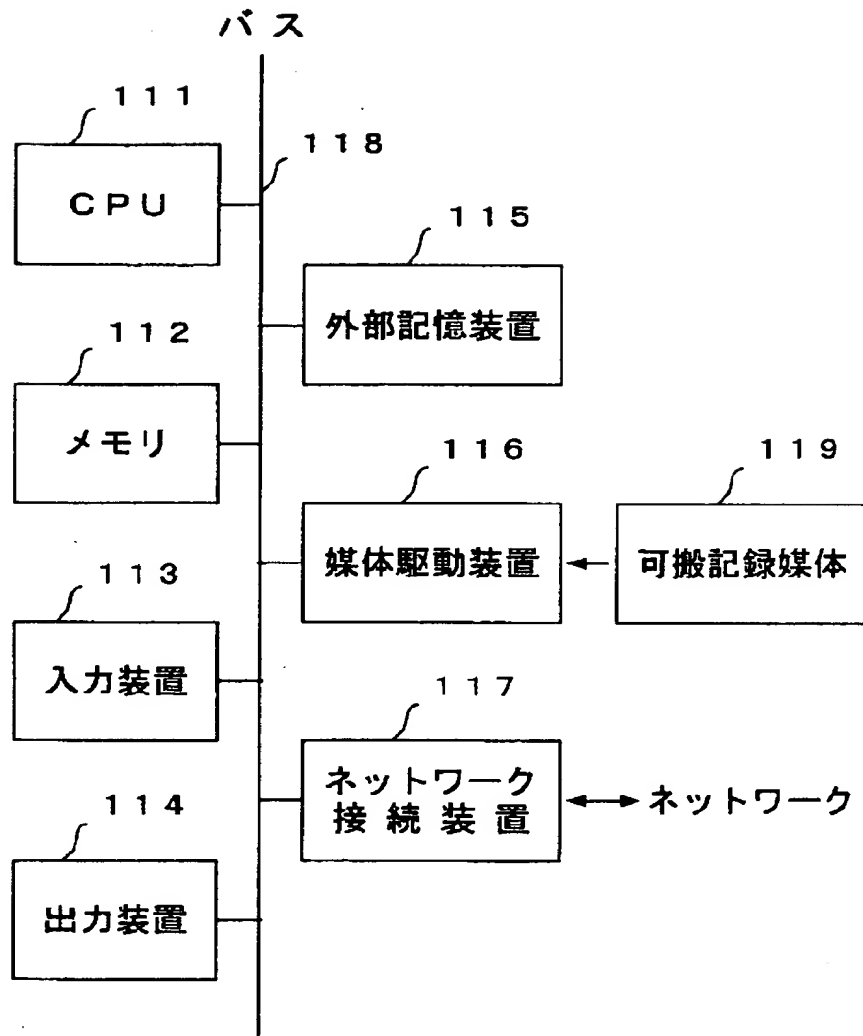
【図 2 6】

加入者カウントテーブルを示す図

証明書 Ser. No.
User 0001
User 0005
User 0068
⋮

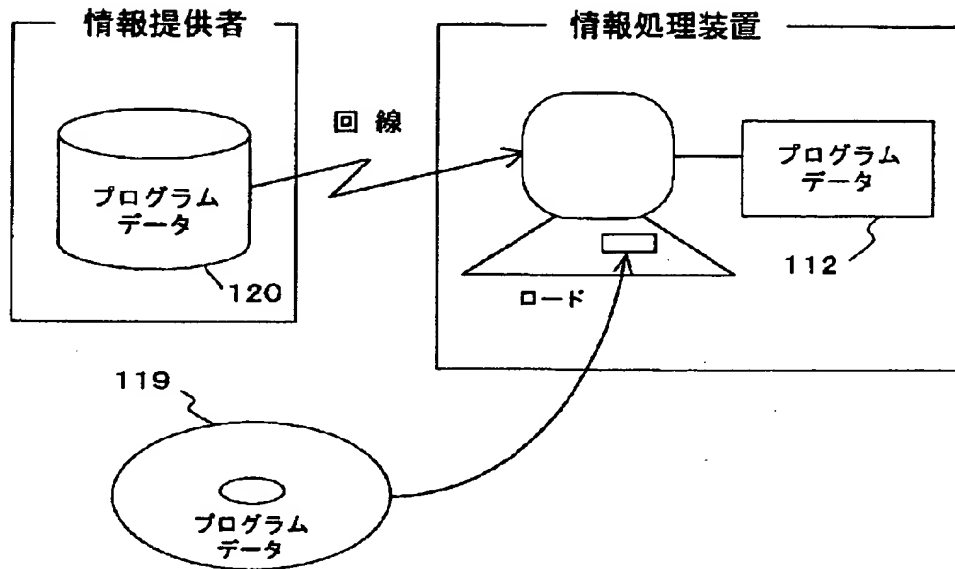
【図27】

情報処理装置の構成図



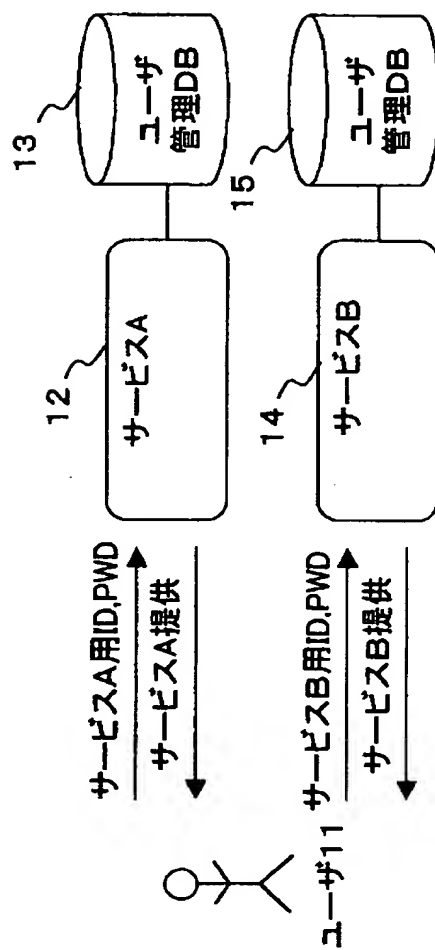
【図 28】

記 録 媒 体 を 示 す 図



【図29】

従来のサービスシステムを示す図



【書類名】 要約書

【要約】

【課題】 ユーザが複数の会員制サービスを利用する場合に、各サービスの入会審査に関する処理を効率化することが課題である。

【解決手段】 サーバ 4 2 のサービス管理 DB 5 2 には、複数のサービスの加入条件が蓄積される。証明書管理部 5 1 は、各サービスの加入条件に基づき、複数のサービスの中からユーザが利用できるサービスを選別して表示する。また、各サービスのサーバに代わって、入会希望ユーザが既に加入している他のサービスの情報を参照することで、そのユーザの入会審査を行う。さらに、各サービスの加入条件に基づいて、新たな加入条件とユーザ数の関係のシミュレーションを行う。

【選択図】 図 1 0

出 願 人 履 歴 情 報

識別番号 [000005223]

1. 変更年月日 1996年 3月26日

[変更理由] 住所変更

住 所 神奈川県川崎市中原区上小田中4丁目1番1号
氏 名 富士通株式会社